Códigos electrónicos

Código de Derecho de la Ciberseguridad

Edición actualizada a 21 de julio de 2016

INCIBE

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/legislacion/codigos/

Alertas de actualización en BOE a la Carta: www.boe.es/a_la_carta/

NIPO (PDF): 007-16-125-9
NIPO (Papel): 007-16-124-3
NIPO (ePUB): 007-16-126-4
ISBN: 978-84-340-2330-7
Depósito Legal: M-25852-2016

Catálogo de Publicaciones de la Administración General del Estado
publicacionesoficiales.boe.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
tel. 911 114 000 – www.boe.es

SUMARIO

NORMATIVA DE SEGURIDAD

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

TELECOMUNICACIONES Y USUARIOS

CIBERDELINCUENCIA

PROTECCIÓN DE DATOS

Índice Sistemático

INFRAESTRUCTURAS CRÍTICAS

NORMATIVA DE SEGURIDAD

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

TELECOMUNICACIONES Y USUARIOS

CIBERDELINCUENCIA

PROTECCIÓN DE DATOS

§ 1

Nota del autor

Última modificación: 19 de julio de 2016

Promovida por el Consejo de Seguridad Nacional, en el año 2013 se publicó la Estrategia de Seguridad Nacional, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación. El propósito de este documento es el de fijar las directrices generales del uso seguro del ciberespacio a través del impulso de una visión integradora que garantice la seguridad y el progreso de España. Tal objetivo debía alcanzarse a través de la adecuada coordinación y cooperación entre todas las Administraciones Públicas, pero también entre aquellas con el sector privado y con los ciudadanos.

La Estrategia persigue lograr la seguridad del ciberespacio a través del desarrollo y aplicación de una política de ciberseguridad nacional, lo que exige contar con un adecuado marco normativo que proporcione una mayor confianza en el uso de las TIC. Dicho fin no sólo tienen que ver la implantación de un marco nacional de políticas públicas, procedimientos y normas técnicas, sino que alcanza a una necesidad de mantener actualizado el ordenamiento jurídico en una materia como la que ahora nos ocupa.

En particular, el Objetivo III de la citada Estrategia ya se refiere a la necesidad de armonizar las legislaciones nacionales a través del desarrollo y mantenimiento de una regulación sólida y eficaz. Por su parte, el Objetivo IV llama a desarrollar una gestión eficaz de los riesgos derivados del ciberespacio sobre la que poder edificar una sólida cultura de ciberseguridad, para lo cual se requiere lograr que los usuarios tengan una especial sensibilización en cuanto al conocimiento de las herramientas para la protección de su información, sistemas y servicios.

Alineada con la citada Estrategia de Seguridad Nacional de 2013, ese mismo año se publica la Estrategia de Ciberseguridad Nacional, la cual se articula a través de una serie de líneas de acción. A los efectos que aquí nos interesan, las líneas de acción 4 y 6 incluyen una serie de referencias con especial incidencia en los aspectos legales de la ciberseguridad. En particular, la línea de acción 4 contempla una serie de medidas destinadas a integrar en el marco legal español las soluciones a los nuevos problemas relacionados con la ciberseguridad en el ámbito penal, y asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado.

A estos efectos, el Instituto Nacional de Ciberseguridad de España (INCIBE), organismo dependiente de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) del Ministerio de Industria, Energía y Turismo, dentro de las funciones que tienen encomendadas para el desarrollo y aplicación de las políticas de ciberseguridad, propone compilar en este documento toda la legislación española que afecte a la ciberseguridad, al objeto de contribuir a mejorar el conocimiento y facilitar la aplicación de una normativa que afecta a una materia tan importante, pero a su vez tan cambiante.

El carácter transversal de la ciberseguridad hace innecesaria la inclusión en este compendio de todas las normas de naturaleza general o, en otras palabras, no exclusivas de esta materia (por citar algunas, la reciente aprobación de la normativa de protección de datos –Reglamento y Directiva- o las últimas modificaciones del código penal en materia de ciberdelitos), que sí son de referencia necesaria en otros códigos normativos ya existentes. De ahí, en ocasiones, su mera referencia en la presente obra.

Sí merece destacar que en fecha 19 de julio de 2016 se publicó en el DOUE la Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión (comúnmente conocida como "Directiva NIS"), que se trata de un documento imprescindible para conocer las nuevas obligaciones exigidas en el campo de la ciberseguridad, y las competencias otorgadas a algunos de los agentes que intervienen en ella –caso de los CERT- y cuya transposición se abordará desde el Ministerio de Industria, Energía y Turismo a lo largo del año 2016.

En definitiva, a través de este compendio se pretende poner a disposición de todos los profesionales una herramienta donde se puedan encontrar, actualizadas, las normas que afecten directamente a la ciberseguridad, y facilitar así el necesario estudio y análisis de una materia que ya resulta imprescindible para lograr una adecuada protección de empresas, instituciones y ciudadanos dentro de un estado social y democrático de derecho.

Francisco Pérez Bes

Secretario General del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE)

ANEXO

NORMATIVA NO CONSOLIDADA

I - NORMATIVA INTERNACIONAL Y COMUNITARIA

§ 1. Convenio sobre la ciberdelincuencia (Budapest) de 23 de noviembre de 2001.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

§ 2. Protocolo Adicional a la Convención de Budapest del Consejo de Europa sobre persecución de los actos de racismo y xenofobia cometidos a través de internet.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793

§ 3. Convención de Lanzarote del año 2007 del Consejo de Europa sobre abuso y explotación sexual de los menores y pornografía infantil.

https://www.boe.es/buscar/act.php?id=BOE-A-2010-17392

§ 4. Directiva 2011/93/UE sobre abuso, explotación sexual de los menores y pornografía infantil.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2011-82637

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32011L0093

§ 5. Directiva 2013/40/UE sobre ataques a los sistemas de información.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l33193

§ 6. Decisión Marco 2008/919/JAI sobre lucha contra el terrorismo.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82452

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008F0919

§ 7. Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82589

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:jl0013

§ 8. Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81623

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32002L0077

§ 9. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24120

§ 10. Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-80701

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24108h

§ 11. Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-80700

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32002L0021

§ 12. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

§ 13. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32000L0031

§ 14. Convenio 108 del Consejo de Europa sobre Protección de Datos de carácter personal.

https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

§ 15. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

§ 16. REGLAMENTO (UE) Nº 611/2013 DE LA COMISION, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32013R0611

§ 17. Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de 21de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº460/2004.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81184

§ 18. Reglamento (UE) nº 513/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por el que se establece, como parte del Fondo de Seguridad Interior, el instrumento de apoyo financiero a la cooperación policial, la prevención y la lucha contra la delincuencia, y la gestión de crisis y por el que se deroga la Decisión 2007/125/JAI del Consejo.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81034

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0513

§ 19. Reglamento (UE) nº 230/2014 del Parlamento Europeo y del Consejo, de 11 de marzo de 2014, por el que se establece un instrumento en pro de la estabilidad y la paz.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2014-80479

§ 20. Carta de Naciones Unidas.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-1990-27553

II.- NORMATIVA NACIONAL

NORMATIVA DE SEGURIDAD NACIONAL

§ 1. Estrategia de Seguridad Nacional: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

§ 2. Estrategia de Ciberseguridad Nacional: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

§ 2

Constitución Española. [Inclusión parcial]

Cortes Generales
«BOE» núm. 311, de 29 de diciembre de 1978
Última modificación: 27 de septiembre de 2011
Referencia: BOE-A-1978-31229

[. . .]

TÍTULO I

De los derechos y deberes fundamentales

[. . .]

CAPÍTULO SEGUNDO

Derechos y libertades

[. . .]

Sección 1.ª De los derechos fundamentales y de las libertades públicas

[. . .]

Artículo 17.

1. Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley.

2. La detención preventiva no podrá durar más del tiempo estrictamente necesario para la realización de las averiguaciones tendentes al esclarecimiento de los hechos, y, en todo caso, en el plazo máximo de setenta y dos horas, el detenido deberá ser puesto en libertad o a disposición de la autoridad judicial.

3. Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca.

4. La ley regulará un procedimiento de «habeas corpus» para producir la inmediata puesta a disposición judicial de toda persona detenida ilegalmente. Asimismo, por ley se determinará el plazo máximo de duración de la prisión provisional.

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[. . .]

Artículo 24.

1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión.
2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos.

[. . .]

CAPÍTULO TERCERO

De los principios rectores de la política social y económica

Artículo 39.

1. Los poderes públicos aseguran la protección social, económica y jurídica de la familia.
2. Los poderes públicos aseguran, asimismo, la protección integral de los hijos, iguales éstos ante la ley con independencia de su filiación, y de las madres, cualquiera que sea su estado civil. La ley posibilitará la investigación de la paternidad.
3. Los padres deben prestar asistencia de todo orden a los hijos habidos dentro o fuera del matrimonio, durante su minoría de edad y en los demás casos en que legalmente proceda.
4. Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos.

[. . .]

Artículo 51.

1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos.
2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios, fomentarán sus organizaciones y oirán a éstas en las cuestiones que puedan afectar a aquéllos, en los términos que la ley establezca.

3. En el marco de lo dispuesto por los apartados anteriores, la ley regulará el comercio interior y el régimen de autorización de productos comerciales.

[. . .]

§ 3

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional

Jefatura del Estado
«BOE» núm. 233, de 29 de septiembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-10389

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones.

La legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia.

Así, las normas aplicables a los estados de alarma, excepción y sitio, a la Defensa Nacional, a las Fuerzas y Cuerpos de Seguridad, a la protección de la seguridad ciudadana, a la protección de infraestructuras críticas, a la protección civil, a la acción y el servicio exterior del Estado o a la seguridad privada, regulan, junto con la legislación penal y los tratados y compromisos internacionales en los que España es parte, distintos aspectos de la seguridad.

Esta regulación se basa en la asignación de competencias a las distintas autoridades y Administraciones Públicas, y se articula en un modelo tradicional y homologable con los países de nuestro entorno, que se ha demostrado válido hasta ahora y que ha permitido hacer frente a las necesidades de seguridad de una sociedad abierta, libre y democrática como la española.

Sin embargo, en el mundo actual, y en el entorno más previsible para el futuro, los actores y circunstancias que ponen en peligro los niveles de seguridad, se encuentran sujetos a constante mutación, y es responsabilidad de los poderes públicos dotarse de la

normativa, procedimientos y recursos que le permitan responder con eficacia a estos desafíos a la seguridad.

En este contexto aparece el campo de la Seguridad Nacional como un espacio de actuación pública nuevo, enfocado a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad.

En este sentido, la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral.

Este esfuerzo de integración reviste tanta mayor importancia cuanto que la Seguridad Nacional debe ser considerada un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte.

Por otro lado, la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el ciberespacio y la estabilidad económica.

La dimensión que adquieren ciertos riesgos y amenazas, su acusada transversalidad, o la combinación de estos rasgos con su naturaleza abierta e incierta, como sucede en las situaciones de interés para la Seguridad Nacional definidas por la presente ley, son factores que indican claramente que toda respuesta que implique a los distintos agentes e instrumentos de la Seguridad Nacional se verá reforzada y resultará más eficiente si se realiza de forma coordinada.

El superior interés nacional requiere mejorar la coordinación de las diferentes Administraciones Públicas, buscando marcos de prevención y respuesta que ayuden a resolver los problemas que plantea una actuación compartimentada, organizando a diversos niveles y de manera integral, la acción coordinada de los agentes e instrumentos al servicio de la Seguridad Nacional.

Esta ley se dicta con el propósito de responder a esta demanda, que viene siendo expresada por los agentes de la Seguridad Nacional integrados en las Administraciones Públicas, por el sector privado y por la sociedad en general. No afecta a la regulación de los distintos agentes e instrumentos que ya son objeto de normas sectoriales específicas, sino que facilita su inserción armónica en el esquema de organización general, establecido por la Estrategia de Seguridad Nacional, de 31 de mayo de 2013, bajo la denominación de Sistema de Seguridad Nacional, y liderado por el Presidente del Gobierno.

II

Esta ley se estructura en cinco títulos.

En el título preliminar, además de las disposiciones relativas a su objeto y ámbito, la ley establece las definiciones y principios generales que inspiran el concepto de Seguridad Nacional como Política de Estado, la Cultura de Seguridad Nacional, la cooperación con las Comunidades Autónomas, la colaboración privada, los componentes fundamentales, así como los ámbitos de especial interés y sus obligaciones.

En el título I se detallan cuáles son los órganos competentes de la Seguridad Nacional y qué competencias se les asignan en esta materia.

Por su parte, el título II se dedica a la creación y definición del Sistema de Seguridad Nacional, sus funciones y organización.

El título III regula la gestión de crisis, como marco general de funcionamiento del Sistema de Seguridad Nacional, y establece definiciones y competencias en dicha materia. La regulación de la situación de interés para la Seguridad Nacional prevé que no se ejerzan en ella las potestades propias de los estados de alarma y de excepción, de modo que si ello fuere necesario habría que proceder a su declaración y al sometimiento a su normativa específica.

Por último, el título IV regula la contribución de recursos a la Seguridad Nacional, que remite a una nueva ley a desarrollar.

La parte final de la ley incluye cuatro disposiciones adicionales sobre coordinación con instrumentos internacionales de gestión de crisis, homologación de instrumentos de gestión de crisis y comunicación pública respectivamente; una disposición transitoria relativa a la actividad de los Comités Especializados existentes a la entrada en vigor de esta ley; y cuatro disposiciones finales, que regulan los títulos competenciales, el desarrollo reglamentario, el mandato legislativo y la entrada en vigor.

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto.*

Esta ley tiene por objeto regular:

a) Los principios básicos, órganos superiores y autoridades y los componentes fundamentales de la Seguridad Nacional.

b) El Sistema de Seguridad Nacional, su dirección, organización y coordinación.

c) La gestión de crisis.

d) La contribución de recursos a la Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. Esta ley será de aplicación a las diferentes Administraciones Públicas y, en los términos que en ella se establecen, a las personas físicas o jurídicas.

2. Los estados de alarma y excepción, se rigen por su normativa específica.

Artículo 3. *Seguridad Nacional.*

A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos.

Artículo 4. *Política de Seguridad Nacional.*

1. La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.

2. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.

3. La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley.

Artículo 5. *Cultura de Seguridad Nacional.*

1. El Gobierno promoverá una cultura de Seguridad Nacional que favorezca la implicación activa de la sociedad en su preservación y garantía, como requisito

indispensable para el disfrute de la libertad, la justicia, el bienestar, el progreso y los derechos de los ciudadanos.

2. A los efectos del número anterior, el Gobierno pondrá en marcha acciones y planes que tengan por objeto aumentar el conocimiento y la sensibilización de la sociedad acerca de los requerimientos de la Seguridad Nacional, de los riesgos y amenazas susceptibles de comprometerla, del esfuerzo de los actores y organismos implicados en su salvaguarda y la corresponsabilidad de todos en las medidas de anticipación, prevención, análisis, reacción, resistencia y recuperación respecto a dichos riesgos y amenazas.

Artículo 6. *Cooperación con las Comunidades Autónomas.*

1. La cooperación entre el Estado y las Comunidades Autónomas en las materias propias de esta ley, se realizará a través de la Conferencia Sectorial para asuntos de la Seguridad Nacional, todo ello sin perjuicio de las funciones asignadas al Consejo de Seguridad Nacional.

2. En particular, corresponderá a la Conferencia, como órgano de cooperación entre el Estado y las Comunidades Autónomas, el tratamiento y resolución con arreglo al principio de cooperación de aquellas cuestiones de interés común relacionadas con la Seguridad Nacional, como las siguientes:

a) Procedimientos técnicos para asegurar la recepción de la información sobre Seguridad Nacional de carácter general por parte de las Comunidades Autónomas, y la articulación de la información que éstas han de aportar al Estado.

b) Fórmulas de participación en los desarrollos normativos sobre Seguridad Nacional, mediante procedimientos internos que faciliten la aplicación de las actuaciones de la política de Seguridad Nacional, así como en la elaboración de los instrumentos de planificación que se prevea utilizar.

c) Problemas planteados en la ejecución de la política de Seguridad Nacional y el marco de las respectivas competencias estatutarias autonómicas.

3. La participación de las Ciudades con Estatuto de Autonomía de Ceuta y Melilla en los asuntos relacionados con la Seguridad Nacional también se articulará en la Conferencia, formando parte de la misma un representante de cada una de ellas.

4. Para su adecuado funcionamiento, la Conferencia elaborará un Reglamento interno. Los acuerdos de la Conferencia se adoptarán conforme a lo dispuesto en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y su Reglamento interno.

Artículo 7. *Colaboración privada.*

1. Las entidades privadas, siempre que las circunstancias lo aconsejen y, en todo caso, cuando sean operadoras de servicios esenciales y de infraestructuras críticas que puedan afectar a la Seguridad Nacional, deberán colaborar con las Administraciones Públicas. El Gobierno establecerá reglamentariamente los mecanismos y formas de esta colaboración.

2. El Gobierno, en coordinación con las Comunidades Autónomas, establecerá cauces que fomenten la participación del sector privado en la formulación y ejecución de la política de Seguridad Nacional.

Artículo 8. *Participación ciudadana en la Seguridad Nacional.*

El Gobierno, en coordinación con las Comunidades Autónomas, establecerá mecanismos que faciliten la participación de la sociedad civil y sus organizaciones en la formulación y la ejecución de la política de Seguridad Nacional.

Artículo 9. *Componentes fundamentales de la Seguridad Nacional.*

1. Se consideran componentes fundamentales de la Seguridad Nacional a los efectos de esta ley la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica.

2. Los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al Sistema de Seguridad Nacional,

proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización.

Artículo 10. *Ámbitos de especial interés de la Seguridad Nacional.*

Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

Artículo 11. *Obligaciones de las Administraciones Públicas en los ámbitos de especial interés.*

1. En el marco del Sistema de Seguridad Nacional, las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional, estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.

2. Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico.

TÍTULO I

Órganos competentes de la Seguridad Nacional

Artículo 12. *Órganos competentes en materia de Seguridad Nacional.*

1. Son órganos competentes en materia de Seguridad Nacional:

a) Las Cortes Generales.
b) El Gobierno.
c) El Presidente del Gobierno.
d) Los Ministros.
e) El Consejo de Seguridad Nacional.
f) Los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla.

2. A los efectos de esta ley, se entenderá que son órganos competentes de las Comunidades Autónomas y de las ciudades con Estatuto de Autonomía de Ceuta y Melilla, los que correspondan según lo dispuesto en cada Estatuto de Autonomía, en relación con las competencias que en cada caso estén relacionadas con la Seguridad Nacional.

3. Las autoridades locales ejercerán las competencias que les corresponden de acuerdo con esta ley y con lo dispuesto en la legislación de régimen local y demás leyes que les sean de aplicación.

Artículo 13. *Las Cortes Generales.*

1. Con independencia de las funciones que la Constitución y las demás disposiciones legales asignan a las Cortes Generales, les corresponde debatir las líneas generales de la política de Seguridad Nacional, a cuyos efectos el Gobierno presentará a las mismas, para su conocimiento y debate, la Estrategia de Seguridad Nacional, así como las iniciativas y planes correspondientes.

2. Se designará en las Cortes Generales una Comisión Mixta Congreso-Senado de Seguridad Nacional, siguiendo para ello lo dispuesto en los reglamentos de las Cámaras,

con el fin de que las Cámaras tengan la participación adecuada en los ámbitos de la Seguridad Nacional y dispongan de la más amplia información sobre las iniciativas en el marco de la política de Seguridad Nacional. En el seno de esta Comisión Mixta comparecerá anualmente el Gobierno, a través del representante que designe, para informar sobre la evolución de la Seguridad Nacional en dicho período de referencia. Asimismo, en esta Comisión Mixta será presentada la Estrategia de Seguridad Nacional y sus revisiones.

Artículo 14. *El Gobierno.*

Corresponde al Gobierno:

a) Establecer y dirigir la política de Seguridad Nacional y asegurar su ejecución.
b) Aprobar la Estrategia de Seguridad Nacional y sus revisiones mediante real decreto, en los términos previstos en esta ley.
c) Efectuar la Declaración de Recursos de Interés para la Seguridad Nacional en coordinación con las Comunidades Autónomas.

Artículo 15. *El Presidente del Gobierno.*

Corresponde al Presidente del Gobierno:

a) Dirigir la política de Seguridad Nacional y el Sistema de Seguridad Nacional.
b) Proponer la Estrategia de Seguridad Nacional y sus revisiones.
c) Declarar la Situación de Interés para la Seguridad Nacional.
d) Ejercer las demás competencias que en el marco del Sistema de Seguridad Nacional le atribuya esta ley, y las demás normas legales y reglamentarias que sean de aplicación.

Artículo 16. *Los Ministros.*

A los Ministros, como responsables de desarrollar la acción del Gobierno en las materias que les son propias, les corresponde desarrollar y ejecutar la política de Seguridad Nacional en los ámbitos de sus respectivos departamentos ministeriales.

Artículo 17. *El Consejo de Seguridad Nacional.*

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan por esta ley y se le asignen por su reglamento.

TÍTULO II

Sistema de Seguridad Nacional

Artículo 18. *El Sistema de Seguridad Nacional.*

1. El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones.
2. En el Sistema de Seguridad Nacional se integran los componentes fundamentales siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada.

Artículo 19. *Funciones.*

Al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis

contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema.

Artículo 20. *Estructura del Sistema de Seguridad Nacional.*

1. El Presidente del Gobierno dirige el Sistema asistido por el Consejo de Seguridad Nacional.

2. El Departamento de Seguridad Nacional ejercerá las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo, así como las demás funciones previstas en la normativa que le sea de aplicación.

3. Los órganos de apoyo del Consejo de Seguridad Nacional, con la denominación de Comités Especializados u otra que se determine, ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen.

4. Será objeto de desarrollo reglamentario, en coordinación con las Administraciones Públicas afectadas, la regulación de los órganos de coordinación y apoyo del Departamento de Seguridad Nacional, así como de los mecanismos de enlace y coordinación permanentes con los organismos de todas las Administraciones del Estado que sean necesarios para que el Sistema de Seguridad Nacional pueda ejercer sus funciones y cumplir sus objetivos; todo ello sin perjuicio de las previsiones que en materia de gestión de crisis se contienen en el título III.

Artículo 21. *Funciones y composición del Consejo de Seguridad Nacional.*

1. Corresponde al Consejo de Seguridad Nacional ejercer las siguientes funciones:

a) Dictar las directrices necesarias en materia de planificación y coordinación de la política de Seguridad Nacional.

b) Dirigir y coordinar las actuaciones de gestión de situaciones de crisis en los términos previstos en el título III.

c) Supervisar y coordinar el Sistema de Seguridad Nacional.

d) Verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y promover e impulsar sus revisiones.

e) Promover e impulsar la elaboración de las estrategias de segundo nivel que sean necesarias y proceder, en su caso, a su aprobación, así como a sus revisiones periódicas.

f) Organizar la contribución de recursos a la Seguridad Nacional conforme a lo establecido en esta ley.

g) Aprobar el Informe Anual de Seguridad Nacional antes de su presentación en las Cortes Generales.

h) Acordar la creación y el fortalecimiento de los órganos de apoyo necesarios para el desempeño de sus funciones.

i) Impulsar las propuestas normativas necesarias para el fortalecimiento del Sistema de Seguridad Nacional.

j) Realizar las demás funciones que le atribuyan las disposiciones legales y reglamentarias que sean de aplicación.

2. A propuesta del Presidente del Gobierno, el Consejo de Seguridad Nacional informará al Rey al menos una vez al año. Cuando el Rey asista a las reuniones del Consejo, lo presidirá.

3. La composición del Consejo de Seguridad Nacional se determinará conforme a lo previsto en el apartado 8 de este artículo. En todo caso, deberán formar parte de dicho Consejo:

a) El Presidente del Gobierno, que lo presidirá.

b) Los Vicepresidentes del Gobierno, si los hubiere.

c) Los Ministros de Asuntos Exteriores y de Cooperación, de Justicia, de Defensa, de Hacienda y Administraciones Públicas, del Interior, de Fomento, de Industria, Energía y Turismo, de Presidencia, de Economía y Competitividad y de Sanidad, Servicios Sociales e Igualdad.

d) El Director del Gabinete de la Presidencia del Gobierno, el Secretario de Estado de Asuntos Exteriores, el Jefe de Estado Mayor de la Defensa, el Secretario de Estado de Seguridad y el Secretario de Estado-Director del Centro Nacional de Inteligencia.

4. El Director del Departamento de Seguridad Nacional será convocado a las reuniones del Consejo de Seguridad Nacional.

5. También podrán formar parte del Consejo, cuando sean convocados en función de los asuntos a tratar, los titulares de los demás departamentos ministeriales y las autoridades autonómicas afectadas en la toma de decisiones y actuaciones a desarrollar por parte del Consejo.

6. Sin perjuicio de lo establecido en los apartados 3 y 4, los titulares de los órganos superiores y directivos de la Administración General del Estado, de los organismos públicos, de las Comunidades Autónomas y de las ciudades con Estatuto de Autonomía, así como las autoridades de la Administración Local, serán convocados a las reuniones del Consejo cuando su contribución se considere necesaria, y en todo caso cuando los asuntos a tratar afecten a sus respectivas competencias.

7. Igualmente podrán ser convocadas aquellas personas físicas o jurídicas cuya contribución se considere relevante a la vista de los asuntos a tratar en el orden del día.

8. Mediante real decreto acordado en Consejo de Ministros, a propuesta del Presidente del Gobierno, se desarrollará la concreta composición, organización y funciones del Consejo de Seguridad Nacional, en el marco de lo dispuesto en esta ley.

TÍTULO III

Gestión de crisis en el marco del Sistema de Seguridad Nacional

Artículo 22. *Gestión de crisis.*

1. La gestión de crisis es el conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios.

2. La gestión de crisis se desarrollará a través de instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación. Su desarrollo será gradual e implicará a los diferentes órganos que componen la estructura del Sistema de Seguridad Nacional, según sus competencias y de acuerdo con la situación de crisis que se produzca. Asimismo, en la gestión de crisis participarán las autoridades de la Comunidad Autónoma que, en su caso, resulte afectada.

Artículo 23. *Situación de interés para la Seguridad Nacional.*

1. La gestión de crisis se desarrollará en la situación de interés para la Seguridad Nacional, adaptándose a las específicas circunstancias de la misma, de acuerdo con lo dispuesto en este título.

2. La situación de interés para la Seguridad Nacional es aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, en los términos previstos en esta ley.

3. La situación de interés para la Seguridad Nacional se afrontará con los poderes y medios ordinarios de las distintas Administraciones Públicas y en ningún caso podrá implicar la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos.

Artículo 24. *Declaración de la situación de interés para la Seguridad Nacional.*

1. La situación de interés para la Seguridad Nacional se declarará por el Presidente del Gobierno mediante real decreto. La declaración incluirá, al menos:

a) La definición de la crisis.
b) El ámbito geográfico del territorio afectado.
c) La duración y, en su caso, posible prórroga.
d) El nombramiento, en su caso, de una autoridad funcional, y la determinación de sus competencias para dirigir y coordinar las actuaciones que procedan.
e) La determinación de los recursos humanos y materiales necesarios para afrontar la situación de interés para la Seguridad Nacional, previstos en los correspondientes planes de preparación y disposición de recursos, así como de otros recursos adicionales que se requieran en cada caso, de acuerdo con lo dispuesto en el título IV.

2. La Declaración de situación de interés para la Seguridad Nacional supondrá la obligación de las autoridades competentes de aportar los medios humanos y materiales necesarios que se encuentren bajo su dependencia, para la efectiva aplicación de los mecanismos de actuación.
3. El Gobierno informará inmediatamente al Congreso de los Diputados de las medidas adoptadas y de la evolución de la situación de interés para la Seguridad Nacional.

Artículo 25. *Funciones del Consejo de Seguridad Nacional en la gestión de crisis.*

1. El Consejo de Seguridad Nacional determinará los mecanismos de enlace y coordinación necesarios para que el Sistema de Seguridad Nacional se active preventivamente y realice el seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional.
2. En la situación de interés para la Seguridad Nacional el Presidente del Gobierno convocará al Consejo de Seguridad Nacional para que ejerza las funciones de dirección y coordinación de la gestión de dicha Situación, todo ello sin perjuicio de la aplicación de la legislación en materia de Defensa Nacional y de las competencias que correspondan al Consejo de Ministros. En los casos en los que el Presidente del Gobierno decida designar una autoridad funcional para el impulso y la gestión coordinada de las actuaciones, el Consejo de Seguridad Nacional asesorará sobre el nombramiento de dicha autoridad.
3. El Consejo de Seguridad Nacional asesorará al Presidente del Gobierno cuando la situación requiera la aplicación de medidas excepcionales previstas en los instrumentos de gestión de crisis de las organizaciones internacionales de las que España sea miembro, todo ello sin perjuicio de las facultades que corresponden al Consejo de Ministros y de lo previsto en la legislación en materia de Defensa Nacional.

Artículo 26. *Órganos de coordinación y apoyo del Consejo de Seguridad Nacional en materia de gestión de crisis.*

1. En materia de gestión de crisis el Consejo de Seguridad Nacional estará asistido por un Comité Especializado de carácter único para el conjunto del Sistema de Seguridad Nacional, para lo cual estará apoyado por el Departamento de Seguridad Nacional. Al citado Comité Especializado le corresponderá, entre otras funciones, elaborar propuestas de las directrices político-estratégicas y formular recomendaciones para la dirección de las situaciones de interés para la Seguridad Nacional. Será presidido por el miembro del Consejo de Seguridad Nacional o en su caso la autoridad funcional, que sea designado por el Presidente del Gobierno.
2. Los instrumentos preventivos de los órganos de coordinación y apoyo del Consejo de Seguridad Nacional podrán activarse anticipadamente, para llevar a cabo el análisis y seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional. A estos efectos, todas las Administraciones y organismos públicos estarán obligados a colaborar de conformidad con lo previsto en esta ley.

TÍTULO IV

Contribución de recursos a la Seguridad Nacional

Artículo 27. *La contribución de recursos a la Seguridad Nacional en el Sistema de Seguridad Nacional.*

1. La aportación de recursos humanos y materiales, tanto públicos como privados, no adscritos con carácter permanente a la Seguridad Nacional, se basará en los principios de contribución gradual y proporcionada a la situación que sea necesario afrontar y de indemnidad.

2. La organización de la contribución de recursos a la Seguridad Nacional recaerá en el Consejo de Seguridad Nacional, en coordinación con las Comunidades Autónomas, en los términos establecidos en esta ley y en las demás que sean de aplicación.

3. Las diferentes Administraciones Públicas, a través de sus órganos competentes, dispondrán de un sistema de identificación, evaluación y planificación de medios y recursos correspondientes a sus respectivos ámbitos competenciales, para hacer frente a los posibles riesgos o amenazas a la Seguridad Nacional.

4. Las Comunidades Autónomas y las Entidades Locales colaborarán en la elaboración de los planes de recursos humanos y materiales necesarios para las situaciones de crisis previstas en esta ley.

5. El sector privado participará en la contribución de recursos a la Seguridad Nacional.

6. El funcionamiento y organización de la contribución de recursos a la Seguridad Nacional se establecerá reglamentariamente de conformidad con lo previsto en esta ley.

Artículo 28. *Catálogo de recursos para la Seguridad Nacional.*

1. El Gobierno, mediante acuerdo del Consejo de Ministros, a propuesta del Consejo de Seguridad Nacional, procederá a aprobar un catálogo de recursos humanos y de medios materiales de los sectores estratégicos de la Nación que puedan ser puestos a disposición de las autoridades competentes en la situación de interés para la Seguridad Nacional. Su elaboración se realizará en coordinación con lo previsto en los catálogos sectoriales existentes en el conjunto de las Administraciones Públicas. A dichos efectos, las Comunidades Autónomas elaborarán los correspondientes catálogos de recursos en base a sus propias competencias y a la información facilitada por el Gobierno, los cuales se integrarán en el mencionado catálogo.

2. Dicho catálogo será actualizado cuando así se establezca por el Gobierno y, en todo caso, cada vez que se revise la Estrategia de Seguridad Nacional, de acuerdo con los nuevos riesgos y amenazas.

3. Una vez aprobado el catálogo, los componentes del Sistema de Seguridad Nacional establecerán las directrices y procedimientos para capacitar a personas y adecuar aquellos medios e instalaciones, públicos y privados, en caso de necesidad. A estos efectos, se elaborarán los planes de preparación y disposición de recursos para la Seguridad Nacional.

Artículo 29. *Declaración de recursos para la Seguridad Nacional.*

1. El Gobierno aprobará mediante real decreto la Declaración de Recursos que se podrán emplear en la situación de interés para la Seguridad Nacional prevista en esta ley. Dicho real decreto incluirá la relación de medios humanos y materiales, tanto públicos como privados, que procedan.

2. La disposición de recursos se efectuará mediante la adscripción al Sistema de Seguridad Nacional del personal, instalaciones y medios, según los planes activados para la situación de interés para la Seguridad Nacional prevista en esta ley. La adscripción de dichos recursos se realizará tal y como se establezca reglamentariamente, en coordinación con las Comunidades Autónomas.

3. Cualquier perjuicio que se ocasione como consecuencia de la declaración de recursos para la Seguridad Nacional dará lugar a la correspondiente indemnización, de acuerdo con lo

dispuesto en las normas legales que resulten de aplicación y, en concreto, en los artículos 139 y siguientes de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición adicional primera.

Los instrumentos de gestión de crisis y de la contribución de recursos del Sistema de Seguridad Nacional servirán de apoyo en los estados de alarma y de excepción de conformidad con su propia regulación específica, a decisión del Gobierno, y sin perjuicio de lo dispuesto en la legislación de Defensa nacional.

Disposición adicional segunda. *Coordinación con otros instrumentos internacionales de gestión de crisis.*

Las normas y procedimientos de gestión de crisis del Sistema de Seguridad Nacional deberán ser compatibles y homologables con los instrumentos de gestión de crisis de las organizaciones internacionales en las que España es parte.

Disposición adicional tercera. *Homologación de los instrumentos de gestión de crisis.*

Los órganos competentes de las distintas Administraciones públicas revisarán, en el plazo de seis meses desde la entrada en vigor de esta ley, sus normas y procedimientos de actuación para adecuar y coordinar su funcionamiento en el Sistema de Seguridad Nacional.

Disposición adicional cuarta. *Comunicación pública.*

El Sistema de Seguridad Nacional deberá contar con una política informativa para situaciones de crisis, cuya coordinación estará a cargo de la autoridad que ejerza de Portavoz del Gobierno.

Disposición transitoria única. *Actividad de los Comités Especializados existentes a la entrada en vigor de esta ley y procedimientos de actuación.*

1. Los Comités Especializados del Consejo de Seguridad Nacional existentes a la entrada en vigor de esta ley, continuarán desarrollando sus funciones de acuerdo con los respectivos acuerdos de constitución hasta que sean adaptados a lo dispuesto en esta ley, lo cual deberá hacerse en el plazo de tres meses desde su entrada en vigor.
2. En particular, en este proceso de adaptación de los acuerdos de constitución de los Comités Especializados mencionados en el apartado anterior, se impulsará la adaptación o preparación de los procedimientos necesarios para coordinar sus actuaciones con cuantos otros órganos colegiados o grupos dependientes de estos confluyan en la gestión de crisis, en el marco de lo previsto en los artículos 18.2 y 22.

Disposición final primera. *Títulos competenciales.*

Esta ley se dicta al amparo de lo dispuesto en el artículo 149.1.4.ª y 29.ª de la Constitución que atribuyen al Estado la competencia exclusiva en materia de defensa y Fuerzas Armadas y en materia de seguridad pública.

Disposición final segunda. *Desarrollo reglamentario.*

Se faculta al Gobierno y a los titulares de los departamentos ministeriales, en el ámbito de sus respectivas competencias, para dictar cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta ley.

Disposición final tercera. *Mandato legislativo.*

El Gobierno, en el plazo de un año desde la entrada en vigor de esta ley, deberá remitir al Congreso de los Diputados un proyecto de ley reguladora de la preparación y disposición de la contribución de recursos a la Seguridad Nacional.

Disposición final cuarta. *Entrada en vigor.*

La presente ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 4

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 4 de noviembre de 2015
Referencia: BOE-A-2010-1330

I

La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En el ámbito de las Administraciones públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del sector privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse

efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.

En este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

II

El Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre Administración electrónica, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, Centro Criptológico Nacional, sociedad de la información, reutilización de la información en el sector público y órganos colegiados responsables de la Administración Electrónica; así como la regulación de diferentes instrumentos y servicios de la Administración, las directrices y guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.

La Ley 11/2007, de 22 de junio, posibilita e inspira esta norma, a cuyo desarrollo coadyuva, en los aspectos de la seguridad de los sistemas de tecnologías de la información en las Administraciones públicas, contribuyendo al desarrollo de un instrumento efectivo que permite garantizar los derechos de los ciudadanos en la Administración electrónica.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal. Además, aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, referente legal imprescindible de cualquier regulación administrativa, determina la configuración de numerosos ámbitos de confidencialidad administrativos, diferentes a la información clasificada y a los datos de carácter personal, que necesitan ser materialmente protegidos. Asimismo determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones realizadas por vía electrónica.

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público que determina la regulación básica del régimen jurídico aplicable a la reutilización de documentos elaborados en el sector público, que configura un ámbito excepcionado de su aplicación, en el que se encuentra la información a la que se refiere el Esquema Nacional de Seguridad.

Junto a las disposiciones indicadas, han inspirado el contenido de esta norma, documentos de la Administración en materia de seguridad electrónica, tales como los Criterios de Seguridad, Normalización y Conservación, las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones, la Metodología y herramientas de análisis y gestión de riesgos o el Esquema Nacional de Interoperabilidad, también desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio.

III

Este real decreto se limita a establecer los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información

de las Administraciones públicas en el ámbito de la Ley 11/2007, de 22 de junio. Con ello, se logra un común denominador normativo, cuya regulación no agota todas las posibilidades de normación, y permite ser completada, mediante la regulación de los objetivos, materialmente no básicos, que podrán ser decididos por políticas legislativas territoriales.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el presente real decreto, se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional, se incluye un glosario de términos y se hace una referencia expresa a la formación.

La norma se estructura en diez capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria y tres disposiciones finales. A los cuatro primeros anexos dedicados a la categoría de los sistemas, las medidas de seguridad, la auditoría de la seguridad, y el glosario de términos, se les une un quinto que establece un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes.

En este real decreto se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. La información tratada en los sistemas electrónicos a los que se refiere este real decreto estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42 apartado 3 y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo, se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.

2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Artículo 2. *Definiciones y estándares.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de Términos incluido en el anexo IV.

Artículo 3. *Ámbito de aplicación.*

El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Artículo 5. *La seguridad como un proceso integral.*

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Artículo 6. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Artículo 7. *Prevención, reacción y recuperación.*

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 8. *Líneas de defensa.*

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 9. *Reevaluación periódica.*

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Artículo 10. *La seguridad como función diferenciada.*

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Requisitos mínimos

Artículo 11. *Requisitos mínimos de seguridad.*

1.Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

2. A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.

Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan.

3. Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán de acuerdo con lo establecido en el artículo 27.

Artículo 12. *Organización e implantación del proceso de seguridad.*

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Artículo 13. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 14. *Gestión de personal.*

1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

2. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

3. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

4. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Artículo 15. *Profesionalidad.*

1. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

2. El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

3. Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Artículo 16. *Autorización y control de los accesos.*

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Artículo 17. *Protección de las instalaciones.*

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Artículo 18. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

4. Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en el artículo 15.

Artículo 19. *Seguridad por defecto.*

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Artículo 20. *Integridad y actualización del sistema.*

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Artículo 21. *Protección de información almacenada y en tránsito.*

1. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Artículo 22. *Prevención ante otros sistemas de información interconectados.*

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Artículo 23. *Registro de actividad.*

Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Artículo 24. *Incidentes de seguridad.*

1. Se establecerá un sistema de detección y reacción frente a código dañino.

2. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 25. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Artículo 26. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Artículo 27. *Cumplimiento de requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

a) Los activos que constituyen el sistema.
b) La categoría del sistema, según lo previsto en el artículo 43.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

3. Los medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

4. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.

5. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad.

Artículo 28. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el presente real decreto en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.

Artículo 29. *Instrucciones técnicas de seguridad y guías de seguridad.*

1. Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

2. El Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Para la redacción y mantenimiento de las

instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

3. Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación.

Artículo 30. *Sistemas de información no afectados.*

Las Administraciones públicas podrán determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el presente de real decreto por tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.

CAPÍTULO IV

Comunicaciones electrónicas

Artículo 31. *Condiciones técnicas de seguridad de las comunicaciones electrónicas.*

1. Las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, según lo establecido en la Ley 11/2007, de 22 de junio, serán implementadas de acuerdo con lo establecido en el Esquema Nacional de Seguridad.

2. Las comunicaciones realizadas en los términos indicados en el apartado anterior, tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte de aplicación.

Artículo 32. *Requerimientos técnicos de notificaciones y publicaciones electrónicas.*

1. Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas:

a) Aseguren la autenticidad del organismo que lo publique.

b) Aseguren la integridad de la información publicada.

c) Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.

d) Aseguren la autenticidad del destinatario de la publicación o notificación.

Artículo 33. *Firma electrónica.*

1. Los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de esta norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en el Esquema Nacional de Interoperabilidad.

2. La política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia.

CAPÍTULO V

Auditoría de la seguridad

Artículo 34. *Auditoría de la seguridad.*

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

2. Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.

3. En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.

4. En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

6. Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

7. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

8. Los informes de auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las tecnologías de la información.

CAPITULO VI

Estado de seguridad de los sistemas

Artículo 35. *Informe del estado de la seguridad.*

El Comité Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente Real Decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado.

CAPÍTULO VII

Respuesta a incidentes de seguridad

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y

de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes de auditoría de los sistemas afectados, registros de auditoría, configuraciones y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquél, será coordinador a nivel público estatal.

CAPÍTULO VIII

Normas de conformidad

Artículo 38. *Sedes y registros electrónicos.*

La seguridad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Seguridad.

Artículo 39. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 40. *Mecanismos de control.*

Cada órgano de la Administración pública o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del Esquema Nacional de Seguridad.

Artículo 41. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

CAPÍTULO IX

Actualización

Artículo 42. *Actualización permanente.*

El Esquema Nacional de Seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y nuevos estándares internacionales sobre seguridad y auditoría en los sistemas y tecnologías de la información y a medida que vayan consolidándose las infraestructuras que le apoyan.

CAPÍTULO X

Categorización de los sistemas de información

Artículo 43. *Categorías.*

1. La categoría de un sistema de información, en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.
2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.
3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Artículo 44. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 43, así como la modificación posterior, en su caso, corresponderá, dentro del ámbito de su actividad, al responsable de cada información o servicio.
2. La facultad para determinar la categoría del sistema corresponderá al responsable del mismo.

Disposición adicional primera. *Formación.*

El personal de las Administraciones públicas recibirá, de acuerdo con lo previsto en la disposición adicional segunda de la Ley 11/2007, de 22 de junio, la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Seguridad, a cuyo fin los órganos responsables dispondrán lo necesario para que la formación sea una realidad efectiva.

Disposición adicional segunda. *Comité de Seguridad de la Información de las Administraciones Públicas.*

El Comité de Seguridad de la Información de las Administraciones Públicas, dependiente del Comité Sectorial de Administración electrónica, contará con un representante de cada una de las entidades presentes en dicho Comité Sectorial. Tendrá funciones de cooperación en materias comunes relacionadas con la adecuación e implantación de lo previsto en el Esquema Nacional de Seguridad y en las normas, instrucciones, guías y recomendaciones dictadas para su aplicación.

Disposición adicional tercera. *Modificación del Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.*

Se modifica la letra b) del apartado 5 del artículo 81 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal aprobado por Real Decreto 1720/2007, de 21 de diciembre, que pasa a tener la siguiente redacción:

«b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.»

Disposición adicional cuarta. *Desarrollo del Esquema Nacional de Seguridad.*

1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.
c) Auditoría de la seguridad.
d) Conformidad con el Esquema Nacional de Seguridad.
e) Adquisición de productos de seguridad.
f) Criptología de empleo en el Esquema Nacional de Seguridad.
g) Interconexión en el Esquema Nacional de Seguridad.
h) Requisitos de seguridad en entornos externalizados.

2. La aprobación de estas instrucciones se realizará de acuerdo con el procedimiento establecido en el citado artículo 29 apartados 2 y 3.

Disposición transitoria. *Adecuación de sistemas.*

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXOS

ANEXO I

Categorías de los sistemas

1. Fundamentos para la determinación de la categoría de un sistema.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el presente real decreto, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

2. Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Disponibilidad [D].
b) Autenticidad [A].
c) Integridad [I].
d) Confidencialidad [C].
e) Trazabilidad [T].

3. Determinación del nivel requerido en una dimensión de seguridad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño menor por los activos de la organización.

3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

2.º El sufrimiento de un daño significativo por los activos de la organización.

3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.º El incumplimiento grave de alguna ley o regulación.

4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de un sistema sobre la base de lo indicado en el apartado anterior no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

5. Secuencia de actuaciones para determinar la categoría de un sistema:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3.

2. Determinación de la categoría del sistema, según lo establecido en el apartado 4.

ANEXO II

Medidas de seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.

b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.
e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.
3. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.
4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad, es la que se indica en la tabla siguiente:

«Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad

«Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Acceso remoto *(remote login)*
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidentes
T	aplica	+	++	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidentes
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	aplica	=	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	aplica	+	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica

«Dimensiones				Medidas de seguridad	
Afectadas	B	M	A		
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	aplica	=	=	mp.info.9	Copias de seguridad *(backup)*
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	+	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos»

En las tablas del presente Anexo se emplean las siguientes convenciones:

a) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz «aplica».

b) «n.a.» significa «no aplica».

c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo «=».

d) Para indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad, se utilizan los signos «+» y «++».

e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

f) En las tablas del presente anexo se han empleado colores verde, amarillo y rojo de la siguiente forma: el color verde para indicar que una cierta medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría MEDIA o superior; el rojo para indicar las medidas que sólo son de aplicación en categoría ALTA.

3. Marco organizativo [org]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.

b) El marco legal y regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que describan:

a) El uso correcto de equipos, servicios e instalaciones.
b) Lo que se considerará uso indebido.
c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que detallen de forma clara y precisa:

a) Cómo llevar a cabo las tareas habituales.
b) Quién debe hacer cada tarea.
c) Cómo identificar y reportar comportamientos anómalos.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

a) Utilización de instalaciones, habituales y alternativas.
b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.
c) Entrada de aplicaciones en producción.
d) Establecimiento de enlaces de comunicaciones con otros sistemas.
e) Utilización de medios de comunicación, habituales y alternativos.
f) Utilización de soportes de información.
g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.
h) Utilización de servicios de terceros, bajo contrato o Convenio.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:

a) Identifique los activos más valiosos del sistema.
b) Identifique las amenazas más probables.
c) Identifique las salvaguardas que protegen de dichas amenazas.
d) Identifique los principales riesgos residuales.

Categoría MEDIA

Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas más probables.
c) Identifique y valore las salvaguardas que protegen de dichas amenazas.
d) Identifique y valore el riesgo residual.

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas posibles.
c) Identifique las vulnerabilidades habilitantes de dichas amenazas.
d) Identifique y valore las salvaguardas adecuadas.
e) Identifique y valore el riesgo residual.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	+

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

Categoría BÁSICA

a) Documentación de las instalaciones:

1. Áreas.
2. Puntos de acceso.

b) Documentación del sistema:

1. Equipos.
2. Redes internas y conexiones al exterior.
3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:

1. Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet o redes públicas en general.
2. Cortafuegos, DMZ, etc.
3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:

1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
2. Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Categoría MEDIA

e) Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Categoría ALTA

f) Sistema de gestión de seguridad de la información con actualización y aprobación periódica.
g) Controles técnicos internos:

1. Validación de datos de entrada, salida y datos intermedios.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

a) Atenderá a las conclusiones del análisis de riesgos: [op.pl.1].
b) Será acorde a la arquitectura de seguridad escogida: [op.pl.2].
c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

4.1.4 Dimensionamiento / gestión de capacidades [op.pl.4].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubrirá los siguientes aspectos:

a) Necesidades de procesamiento.
b) Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
d) Necesidades de comunicación.
e) Necesidades de personal: cantidad y cualificación profesional.
f) Necesidades de instalaciones y medios auxiliares.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Categoría ALTA

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.
Una instrucción técnica de seguridad detallará los criterios exigibles.

4.2 Control de acceso. [op.acc].

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.
El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.
En todo control de acceso se requerirá lo siguiente:

a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].

c) Que la utilización de los recursos esté protegida [op.acc.2].

d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].

e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].

f) Que la identidad de la entidad quede suficientemente autenticada [mp.acc.5].

g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.

2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.

3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:

a) Se puede saber quién recibe y qué derechos de acceso recibe.

b) Se puede saber quién ha hecho algo y qué ha hecho.

4. Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.

5. En los supuestos contemplados en el Capítulo IV relativo a "Comunicaciones Electrónicas", las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE:

– Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento n.º 910/2014)

– Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento n.º 910/2014)
– Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento n.º 910/2014).

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Los requisitos de acceso se atenderán a lo que a continuación se indica:

a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	I C A T		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.
En concreto, se separarán al menos las siguientes funciones:

a) Desarrollo de operación.
b) Configuración y mantenimiento del sistema de operación.
c) Auditoría o supervisión de cualquier otra función.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.
b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

4.2.5 Mecanismo de autenticación [op.acc.5].

dimensiones	ICAT		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

– "algo que se sabe": contraseñas o claves concertadas.
– "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, *tokens).*
– "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

– Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
– De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
– De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
c) Se atenderá a la seguridad de las credenciales de forma que:

1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) Se exigirá el uso de al menos dos factores de autenticación.
b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:

1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

a) Las credenciales se suspenderán tras un periodo definido de no utilización.
b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

4.2.6 Acceso local [op.acc.6].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización. Estos accesos tendrán en cuenta el nivel de las dimensiones de seguridad:

Nivel BAJO

a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable).
b) El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.
c) Se registrarán los accesos con éxito, y los fallidos.
d) El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

Nivel MEDIO

Se informará al usuario del último acceso efectuado con su identidad.

Nivel ALTO

a) El acceso estará limitado por horario, fechas y lugar desde donde se accede.
b) Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

4.2.7 Acceso remoto [op.acc.7].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	=

Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.
Nivel BAJO
Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (como [op.acc.6]) como el canal de acceso remoto (como en [mp.com.2] y [mp.com.3]).

Nivel MEDIO

Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se configurarán los equipos previamente a su entrada en operación, de forma que:

a) Se retiren cuentas y contraseñas estándar.
b) Se aplicará la regla de «mínima funcionalidad»:

1.º El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,
2.º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
3.º Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.

c) Se aplicará la regla de «seguridad por defecto»:

1.º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
2.º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
3.º El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

4.3.3 Gestión de la configuración [op.exp.3].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

a) Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
b) Se mantenga en todo momento la regla de "seguridad por defecto" ([op.exp.2]).
c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).
d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).
e) El sistema reaccione a incidentes (ver [op.exp.7]).

4.3.4 Mantenimiento [op.exp.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
b) Se efectuará un seguimiento continuo de los anuncios de defectos.

c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware».
Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

a) Procedimiento de reporte de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
d) Procedimientos para informar a las partes interesadas, internas y externas.
e) Procedimientos para:

1. Prevenir que se repita el incidente.
2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

4.3.8 Registro de la actividad de los usuarios [op.exp.8].

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

Se registrarán las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel BAJO

Se activarán los registros de actividad en los servidores.

Nivel MEDIO

Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO

Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
c) Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

4.3.10 Protección de los registros de actividad [op.exp.10].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se protegerán los registros del sistema, de forma que:

a) Se determinará el periodo de retención de los registros.
b) Se asegurará la fecha y hora. Ver [mp.info.5].
c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.
d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

4.3.11 Protección de claves criptográficas [op.exp.11].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	=

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Categoría BÁSICA

a) Los medios de generación estarán aislados de los medios de explotación.
b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Categoría MEDIA

a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5].
b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

4.4 Servicios externos [op.ext].

Cuando se utilicen recursos externos a la organización, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones.
La organización sigue siendo en todo momento responsable de los riesgos en que se incurre en la medida en que impacten sobre la información manejada y los servicios finales prestados por la organización.
La organización dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Para la gestión diaria del sistema, se establecerán los siguientes puntos:

a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.
c) El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres (ver [op.exp.7]).

4.4.3 Medios alternativos [op.ext.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual.

4.5 Continuidad del servicio [op.cont].

4.5.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Se realizará un análisis de impacto que permita determinar:

a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
b) Los elementos que son críticos para la prestación de cada servicio.

4.5.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:

a) Se identificarán funciones, responsabilidades y actividades a realizar.
b) Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
d) Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
e) El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

4.5.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad

4.6 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad.

4.6.1 Detección de intrusión [op.mon.1].

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se dispondrán de herramientas de detección o de prevención de intrusión.

4.6.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:

Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría MEDIA:

Además, se recopilaran datos para valorar el sistema de gestión de incidentes, permitiendo conocer

– Número de incidentes de seguridad tratados.
– Tiempo empleado para cerrar el 50% de los incidentes.
– Tiempo empleado para cerrar el 90% de las incidentes.

Categoría ALTA

Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:

– Recursos consumidos: horas y presupuesto.

5. Medidas de protección [mp]

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El equipamiento de instalará en áreas separadas específicas para su función.

Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El mecanismo de control de acceso se atendrá a lo que se dispone a continuación:

a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.
b) Se registrarán las entradas y salidas de personas.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

a) Condiciones de temperatura y humedad.
b) Protección frente a las amenazas identificadas en el análisis de riesgos.
c) Protección del cableado frente a incidentes fortuitos o deliberados.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+	=

Nivel BAJO

Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos:

a) Se garantizará el suministro de potencia eléctrica.
b) Se garantizará el correcto funcionamiento de las luces de emergencia.

Nivel MEDIO

Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.

5.1.8 Instalaciones alternativas [mp.if.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Cada puesto de trabajo se caracterizará de la siguiente forma:

a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.
b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.
c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

a) Se especificarán las medidas disciplinarias a que haya lugar.

b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

2. En caso de personal contratado a través de un tercero:

a) Se establecerán los deberes y obligaciones del personal.
b) Se establecerán los deberes y obligaciones de cada parte.
c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

5.2.3 Concienciación [mp.per.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.
En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.
b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

5.2.4 Formación [mp.per.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción a incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

5.2.5 Personal alternativo [mp.per.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá estar sometido a las mismas garantías de seguridad que el personal habitual.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	=

Categoría BÁSICA

Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento

Categoría MEDIA

Este material se guardará en lugar cerrado cuando no se esté utilizando.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Nivel ALTO

Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

5.3.3 Protección de portátiles [mp.eq.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

c) Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza.

d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

Categoría ALTA

a) Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.

b) La información de nivel alto almacenada en el disco se protegerá mediante cifrado.

5.3.4 Medios alternativos [mp.eq.9].

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	=

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.

Igualmente, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.

Categoría ALTA

a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

b) Se dispondrán sistemas redundantes.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Nivel ALTO

a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.4.3 Protección de la autenticidad y de la integridad [mp.com.3].

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Nivel BAJO

a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información (ver [op.acc.5]).

b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos:

1. La alteración de la información en tránsito.
2. La inyección de información espuria.
3. El secuestro de la sesión por una tercera parte.

c) Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación.

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

Nivel ALTO

a) Se valorará positivamente el empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
c) Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

5.4.4 Segregación de redes [mp.com.4].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Categoría ALTA
La red se segmentará en segmentos de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.
b) Control de salida de la información disponible en cada segmento.
c) Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como en [mp.com.1]).

5.4.5 Medios alternativos [mp.com.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de medios alternativos de comunicación para el caso de que fallen los medios habituales. Los medios alternativos de comunicación:

a) Estarán sujetos y proporcionar las mismas garantías de protección que el medio habitual.
b) Garantizarán un tiempo máximo de entrada en funcionamiento.

5.5 Protección de los soportes de información [mp.si].

5.5.1 Etiquetado [mp.si.1].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

5.5.2 Criptografía [mp.si.2].

dimensiones	I C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Esta medida se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles, los CD, DVD, discos USB, u otros de naturaleza análoga.

Nivel MEDIO

Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

Nivel ALTO

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.5.3 Custodia [mp.si.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

a) Garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) ó lógicas ([mp.si.2]), o ambas.
b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

5.5.4 Transporte [mp.si.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

a) Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.
b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.
c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.

d) Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.
e) Se gestionarán las claves según [op.exp.11].

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	+	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.
2. Cuando así lo requiera el procedimiento asociado al tipo de información contenida.

c) Se emplearán productos certificados conforme a lo establecido en ([op. pl.5]).

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	bajo	medio	alto
	no aplica	aplica	=

Categoría MEDIA

a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

b) Se aplicará una metodología de desarrollo reconocida que:

1.º Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
2.º Trate específicamente los datos usados en pruebas.
3.º Permita la inspección del código fuente.
4.º Incluya normas de programación segura.

c) Los siguientes elementos serán parte integral del diseño del sistema:

1.º Los mecanismos de identificación y autenticación.
2.º Los mecanismos de protección de la información tratada.
3.º La generación y tratamiento de pistas de auditoría.

d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

a) Se comprobará que:

1.º Se cumplen los criterios de aceptación en materia de seguridad.
2.º No se deteriora la seguridad de otros componentes del servicio.

b) Las pruebas se realizarán en un entorno aislado (pre-producción).
c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.
b) Pruebas de penetración.

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de coherencia en la integración en los procesos.
b) Se considerará la oportunidad de realizar una auditoría de código fuente.

5.7 Protección de la información [mp.info].

5.7.1 Datos de carácter personal [mp.info.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.
Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	+	=

Nivel BAJO

1. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.
2. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
3. La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I.
4. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
5. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Nivel MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Y cualquier otra actividad relacionada con dicha información.

5.7.3 Cifrado de la información [mp.info.3].

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Para el cifrado de información se estará a lo que se indica a continuación:

a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.
b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2].
c) Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en [mp.si.2].

5.7.4 Firma electrónica [mp.info.4].

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.
La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.
En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27.

Nivel BAJO

Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:
d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1. Certificados.
2. Datos de verificación y validación.

e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d).

f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Nivel ALTO

1. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.
2. Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

5.7.5 Sellos de tiempo [mp.info.5].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Los sellos de tiempo prevendrán la posibilidad del repudio posterior:

1. Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
2. Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
3. Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.
4. Se utilizarán productos certificados (según [op.pl.5]) o servicios externos admitidos (véase [op.exp.10]).
5. Se emplearán "sellos cualificados de tiempo electrónicos" acordes con la normativa europea en la materia.

5.7.6 Limpieza de documentos [mp.info.6].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

5.7.7 Copias de seguridad (backup) [mp.info.9].

dimensiones	D

nivel	bajo	medio	alto
	aplica	=	=

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

g) Información de trabajo de la organización.

h) Aplicaciones en explotación, incluyendo los sistemas operativos.

i) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

j) Claves utilizadas para preservar la confidencialidad de la información.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico (e-mail) [mp.s.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».

2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3.º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
nivel	básica	media	alta
	aplica	=	+

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

2.º Se prevendrán ataques de manipulación de URL.

3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies".

4.º Se prevendrán ataques de inyección de código.

b) Se prevendrán intentos de escalado de privilegios.

c) Se prevendrán ataques de "cross site scripting".

d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés".

Nivel BAJO

Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.

Nivel ALTO

Se emplearán "certificados cualificados de autenticación del sitio web" acordes a la normativa europea en la materia.

5.8.3 Protección frente a la denegación de servicio [mp.s.8].

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	+

Nivel MEDIO

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello:

a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.

b) Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO

a) Se establecerá un sistema de detección de ataques de denegación de servicio.

b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

5.8.4 Medios alternativos [mp.s.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales.

6. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

7. Interpretación

La interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas CCN-STIC correspondientes a la implementación y a diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría.

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:

a) Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

2. Niveles de auditoría.

Los niveles de auditoría que se realizan a los sistemas de información, serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o

complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

b) Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación.

La interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la instrucción técnica CCN-STIC correspondiente, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Proceso de seguridad. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Servicios acreditados. Servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

Acrónimos

CCN: Centro Criptológico Nacional.
CERT: Computer Emergency Reaction Team.
INTECO: Instituto Nacional de Tecnologías de la Comunicación.
STIC: Seguridad de las Tecnologías de Información y Comunicaciones.

ANEXO V

Modelo de cláusula administrativa particular

Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 115.4 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes

certificados, recogida en el apartado 4.1.5 del anexo II del citado Real Decreto 3/2010, de 8 de enero.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

§ 5

Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

Ministerio de la Presidencia
«BOE» núm. 230, de 25 de septiembre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-16830

La utilización de las Tecnologías de la Información (TI) en amplias áreas de la actividad de la Administración, así como la creciente participación de España en proyectos de desarrollo de la sociedad de la información de carácter internacional, imponen la necesidad de garantizar un nivel de seguridad en la utilización de las TI equiparable, como mínimo, al conseguido en el tratamiento tradicional de la información en soporte papel.

Por tanto, la seguridad que las TI deben poseer, ha de abarcar la protección de la confidencialidad, la integridad y la disponibilidad de la información que manejan los sistemas de información, así como la integridad y disponibilidad de los propios sistemas.

La garantía de seguridad de las Tecnologías de la Información debe estar basada en el establecimiento de mecanismos y servicios de seguridad, adecuadamente diseñados, que impidan la realización de funciones no deseadas.

Uno de los métodos, admitido internacionalmente, para garantizar la corrección y efectividad de dichos mecanismos y servicios, consiste en la evaluación de la seguridad de las TI, realizada mediante la utilización de criterios rigurosos, con posterior certificación por el organismo legalmente establecido.

El Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que acompaña a esta Orden Ministerial, regula el marco de actuación, y crea los organismos necesarios, para poner estos procesos de evaluación y certificación al alcance de la industria y de la Administración; todo ello basado en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

La carencia actual de un esquema análogo, puede suponer un importante obstáculo para la difusión y aceptación generalizada, tanto a nivel nacional como internacional, de los diferentes productos y sistemas de las Tecnologías de la Información desarrollados en nuestro país.

En el contexto de los programas internacionales, no se puede entender criterios de evaluación y certificación de la seguridad de las TI que no sean homologables con los de otros países participantes. Por ello, es necesario la adopción de criterios internacionales, que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que el Esquema al que se refiere el presente Reglamento, se equipare a los del resto de los países de nuestro entorno.

Desde hace algunos años, en España, se ha venido sintiendo la necesidad de impulsar la creación de un esquema de esta naturaleza, habiéndose llevado a cabo diversas

iniciativas para su constitución, desde el Consejo Superior de Informática y para el Impulso de la Administración Electrónica, en colaboración con el Centro Nacional de Inteligencia. También, en la Dirección General de Armamento y Material del Ministerio de Defensa, se creó un esquema orientado a satisfacer necesidades puntuales del Ministerio de Defensa.

Asimismo, se creó un laboratorio de evaluación, el Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aeroespacial (INTA). Este laboratorio fue acreditado, siguiendo este mismo Reglamento, como laboratorio de evaluación de la seguridad de las Tecnologías de la Información, por resolución 1AO/38272/2005, de 13 de octubre, del Centro Criptológico Nacional, y ha contribuido, de manera decisiva, a la creación y puesta en marcha de un esquema de funcionalidad completa.

Paralelamente, España, como país consumidor de certificados, y a través del Ministerio de Administraciones Públicas, ha estado presente en el Arreglo de Reconocimiento Mutuo de Certificados Common Criteria (CCRA), desde su creación.

En ese Ministerio, se ha sentido la necesidad de crear un único esquema nacional que abarcase todo el ámbito de la actividad de evaluación y certificación y que potenciase a España a la categoría de país productor de certificados Common Criteria.

Por todo ello, la creación de un esquema nacional va a gozar, desde el principio, de aportaciones experimentadas y se va a encajar en un foro en el que su presencia es demandada.

Por otra parte, se hace necesaria la participación de un organismo de certificación, que partiendo de un conocimiento de las Tecnologías de la Información y de las amenazas y vulnerabilidades existentes, proporcione una garantía razonable a los procesos de evaluación y certificación.

Dicho organismo se constituye al amparo de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, que encomienda a este Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información, y según lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, entre cuyas funciones está la de constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

En virtud de los preceptos indicados anteriormente, consultados los fabricantes e importadores del sector, y a propuesta conjunta de los Ministros de Defensa y de Industria, Turismo y Comercio, con la aprobación previa de la Ministra de Administraciones Públicas, dispongo:

Artículo único. *Aprobación del Reglamento.*

Se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, cuyo texto se inserta a continuación.

Disposición adicional única. *Naturaleza y establecimiento de la contraprestación exigida por las acreditaciones y certificaciones.*

1. Al amparo de lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, los ingresos procedentes de las acreditaciones de laboratorios y de las certificaciones de productos, tienen la naturaleza de tasas.

2. Según lo establecido en el artículo 2.3 del Real Decreto 1287/2005, de 28 de octubre, por el que se modifica el Real Decreto 593/2002, de 28 de junio, que desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, el establecimiento o modificación de la cuantía de los ingresos que tengan la naturaleza de tasas, así como la fijación de los diversos elementos de la correspondiente relación jurídico-tributaria, se harán con arreglo a lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

Disposición final primera. *Facultades de ejecución y aplicación.*

Se faculta al Secretario de Estado Director del Centro Criptológico Nacional del Centro Nacional de Inteligencia, para dictar cuantas instrucciones sean necesarias para la ejecución y aplicación de lo establecido en esta orden ministerial.

Disposición final segunda. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente Reglamento tiene por objeto la articulación del Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, respectivamente.

Artículo 2. *Definiciones.*

En el marco del presente Reglamento, los conceptos que a continuación se indican, se entenderán como están definidos.

Acreditación.–Declaración de conformidad de los laboratorios solicitantes, emitida por el Organismo de Certificación, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV, del presente Reglamento.

Acreditación de competencia técnica.–Es aquella acreditación que concede una entidad de acreditación reconocida a un laboratorio, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025. En su alcance se deberán incluir las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información aprobadas por el Organismo de Certificación.

Certificación.–Es la determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto con unos criterios preestablecidos.

Declaración de seguridad.–Conjunto de requisitos y especificaciones de las propiedades de seguridad de un producto o sistema de las Tecnologías de la Información.

Evaluación.–Es el análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las Tecnologías de la Información para proteger las condiciones de la información de acuerdo a unos criterios establecidos, con objeto de determinar si puede ser certificado.

Información de las evaluaciones.–Es todo asunto, acto, documento, dato u objeto relacionado con la actividad de evaluación de la seguridad de un producto. La información de las evaluaciones incluye toda la documentación, programas de ordenador, esquemas, planos y demás datos suministrados por el fabricante, los programas de ordenador, planes, pruebas, análisis y resultados de la evaluación elaborados por el laboratorio, así como toda la documentación administrativa y contractual y las comunicaciones del laboratorio con el fabricante del producto y con el Organismo de Certificación, además de los registros de la actividad del laboratorio, incluyendo los de seguridad.

Producto a evaluar.–Es el producto, sistema de información o perfil de protección para el que se solicita una certificación de sus propiedades de seguridad.

Producto clasificado.–Son aquellos productos con requisitos específicos para manejar con seguridad materias clasificadas, o cuya información de especificación, diseño o

desarrollo está clasificada, incluso parcialmente, según lo dispuesto en la Ley 9/68, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/78, de 7 de octubre.

Laboratorio de evaluación.–Es un laboratorio de ensayo, según se define en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial.

Sistema de información.–Es el conjunto de elementos «hardware», «software», datos y usuarios que, relacionados entre sí, permiten el almacenamiento, transmisión, transformación y recuperación de la información.

Artículo 3. *Ámbito de aplicación.*

El ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema.

También comprende a estas entidades cuando sean fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos, en el marco del Esquema.

Todo ello, siempre que dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

CAPÍTULO II

Estructura y funciones del organismo de certificación

Sección 1.ª Estructura del organismo de certificación

Artículo 4. *Estructura.*

A los efectos de funcionamiento del Organismo de Certificación, su estructura será la siguiente:

a) Director del Organismo de Certificación, que será el Secretario de Estado Director del Centro Criptológico Nacional.

b) Secretario General del Organismo de Certificación, que será el Secretario General del Centro Criptológico Nacional.

c) Subdirector de Certificación, que será un funcionario del Centro Nacional de Inteligencia, con rango de Subdirector General, designado por el Director del Organismo de Certificación.

d) Jefe del Área de Certificación, que será un funcionario del Centro Criptológico Nacional, con rango de Subdirector General Adjunto, designado por el Subdirector de Certificación.

e) Los correspondientes Responsables, Técnico de Certificación, de Calidad, de Seguridad, y de Registro, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

f) Personal técnico de certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

g) Personal de enlace con los servicios de Secretaría, y demás personal de soporte administrativo a las actividades del Organismo de Certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

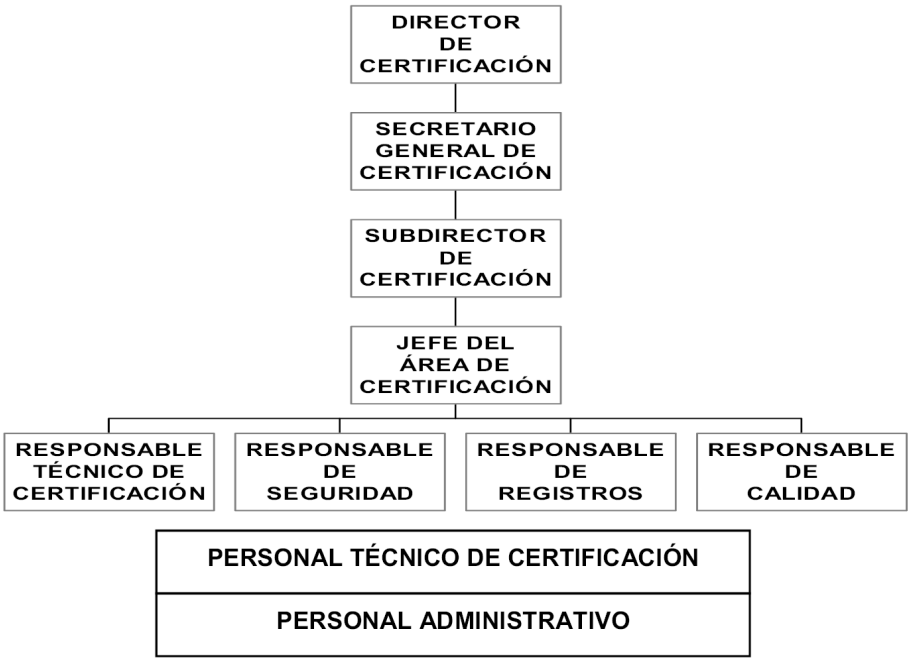


Figura 1. Estructura del Organismo de Certificación

Sección 2.ª Funciones de los cargos del organismo de certificación

Artículo 5. *Director del Organismo de Certificación.*

Corresponde al Director del Organismo de Certificación:

a) Aprobar y hacer cumplir las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación, garantizando la adecuación de la organización y de los medios materiales y humanos a los fines propuestos.

b) Dictar las resoluciones sobre las solicitudes de acreditación de laboratorios y de certificación de la seguridad de productos y sistemas de las Tecnologías de la Información.

c) Establecer los acuerdos oportunos con otros organismos similares en el ámbito de su competencia.

Artículo 6. *Secretario General del Organismo de Certificación.*

Corresponde al Secretario General del Organismo de Certificación:

a) Apoyar y asistir al Director del Organismo de Certificación en el ejercicio de sus funciones.

b) Establecer los mecanismos y sistemas de organización del Organismo de Certificación y determinar las actuaciones precisas para su actualización y mejora.

c) Dirigir el funcionamiento de los servicios comunes del Organismo de Certificación a través de las correspondientes instrucciones y órdenes de servicio.

d) Desempeñar la jefatura superior del personal del Organismo de Certificación, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

Artículo 7. *Subdirector de Certificación.*

Corresponde al Subdirector de Certificación:

a) Presidir el Consejo de Acreditación y Certificación, conforme a lo establecido en el presente Reglamento.

b) Representar al Organismo de Certificación en aquellos foros de índole técnica, de normalización y de divulgación de las actividades del citado organismo, de las normas aplicables y en los de arreglos y acuerdos de reconocimiento mutuo.

c) Revisar las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

d) Proponer los presupuestos y planes de formación anuales del Organismo de Certificación.

Artículo 8. *Jefe del Área de Certificación.*

Corresponde al Jefe del Área de Certificación:

a) Desempeñar la dirección de los servicios técnicos del Organismo de Certificación.

b) Dirigir las instrucciones y procedimientos de acreditación de laboratorios y de certificación de productos.

c) Elevar las correspondientes propuestas de resolución a las mencionadas solicitudes de acreditación y certificación.

d) Instruir, de oficio, los procedimientos de mantenimiento de la acreditación de los laboratorios.

Artículo 9. *Responsable Técnico de Certificación.*

Corresponde al Responsable Técnico de Certificación:

a) Apoyar y asistir al Jefe del Área de Certificación en el ejercicio de sus funciones.

b) Coordinar y dirigir la actuación diaria del personal técnico del Organismo de Certificación.

c) Realizar la asignación de personal técnico a la instrucción de cada solicitud de acreditación de laboratorio y de certificación de producto.

d) Dictaminar las interpretaciones técnicas de normas, métodos y procedimientos de evaluación empleados, bien de oficio, o a instancia de los laboratorios.

e) Elaborar o proponer las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

Artículo 10. *Responsable de Calidad del Organismo de Certificación.*

Corresponde al Responsable de Calidad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la calidad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de calidad, tras su evaluación.

Artículo 11. *Responsable de Seguridad del Organismo de Certificación.*

Corresponde al Responsable de Seguridad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la seguridad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de la seguridad, tras su evaluación.

Artículo 12. *Responsable de Registro del Organismo de Certificación.*

Corresponde al Responsable de Registro del Organismo de Certificación, la gestión y custodia de los registros de calidad, seguridad, certificación y acreditación, manejados por el Organismo de Certificación.

Artículo 13. *Personal técnico del Organismo de Certificación.*

Corresponde al personal técnico del Organismo de Certificación, el desarrollo de la instrucción de los expedientes de acreditación de laboratorio y de certificación de productos,

practicando las pruebas conforme a los medios y procedimientos establecidos por el Organismo de Certificación.

Sección 3.ª Consejo de acreditación y certificación

Artículo 14. *Naturaleza.*

El Consejo de Acreditación y Certificación es un órgano colegiado, distinto e independiente del Organismo de Certificación, regido por lo establecido en el Capítulo II del Título II, de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, por lo establecido en el presente Reglamento.

Artículo 15. *Composición.*

Corresponde al Subdirector de Certificación la presidencia del Consejo de Acreditación y Certificación.

Formarán parte como miembros del Consejo, los siguientes:

a) El Jefe del Área de Certificación, que podrá asumir la presidencia del Consejo por delegación del Subdirector de Certificación.

b) El Responsable Técnico de Certificación, que hará las veces de Secretario del Consejo.

c) Un representante del Ministerio de Defensa, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

d) Un representante del Ministerio de Industria, Turismo y Comercio, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

e) Un representante del Consejo Superior de Administración Electrónica, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Consejo.

f) Un representante de cada laboratorio acreditado, nombrado por dicho laboratorio.

g) Dos representantes de los sectores empresariales de fabricantes, importadores e integradores de productos y sistemas de las Tecnologías de la Información, a propuesta razonada y acordada de dichos sectores.

Artículo 16. *Fines.*

Corresponde al Consejo de Acreditación y Certificación:

a) Vigilar que la normativa del Organismo de Certificación se corresponda y equipare con los términos y referencias de esquemas de certificación equivalentes, que pudieran existir en el ámbito de la Unión Europea en particular, y en el ámbito internacional, en general.

b) Asesorar al Organismo de Certificación en la evolución de sus procedimientos documentados, orientando la gestión de éste, al mejor servicio del tejido industrial y empresarial de fabricantes, importadores e integradores de productos y sistemas de Tecnologías de la Información.

c) Asesorar al Organismo de Certificación en la identificación de esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para la Administración y el sector privado español.

Artículo 17. *Atribuciones.*

Las atribuciones del Consejo de Acreditación y Certificación son las siguientes:

a) Estar permanentemente informado de la normativa que regula el funcionamiento del Organismo de Certificación, incluyendo sus normas de evaluación y certificación, manuales, procedimientos e instrucciones técnicas.

b) Estar permanentemente informado de la relación de laboratorios acreditados y de productos certificados.

c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad de los productos y sistemas de información, con los que el Organismo de

Certificación tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

d) Proponer directrices y recomendaciones al Organismo de Certificación, que serán recogidas en las correspondientes actas de las reuniones del Consejo, a las que deberá dar cumplida respuesta el Director del Organismo de Certificación.

Artículo 18. *Periodicidad de las reuniones.*

El Consejo de Acreditación y Certificación se reunirá, como mínimo, una vez al año, sin perjuicio de que en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

Las reuniones se convocarán a requerimiento del Organismo de Certificación, o por acuerdo del propio Consejo de Acreditación.

Sección 4.ª Acreditación y certificación

Artículo 19. *Acreditación de laboratorios.*

El Organismo de Certificación acredita a los laboratorios solicitantes, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV de este Reglamento.

Artículo 20. *Certificación de productos.*

El Organismo de Certificación certifica la seguridad de los productos y sistemas de Tecnologías de la Información, según lo establecido en el procedimiento del Capítulo V, y atendiendo a los criterios, métodos y normas de evaluación de la seguridad, establecidos en el Capítulo VI.

Artículo 21. *Publicaciones del Esquema.*

El Organismo de Certificación mantendrá actualizada la relación de laboratorios acreditados y la de productos y sistemas de las Tecnologías de la Información certificados. Dicha relación se podrá consultar en la siguiente dirección electrónica: http://www.oc.ccn.cni.es.

CAPÍTULO III

Requisitos de acreditación de laboratorios

Artículo 22. *Requisitos generales para la acreditación de laboratorios.*

1. Para la acreditación de los laboratorios de evaluación de la seguridad de las Tecnologías de la Información se requerirá el cumplimiento de los siguientes requisitos:

a) Capacidad para la evaluación de la seguridad de productos de las Tecnologías de la Información, demostrada mediante la acreditación de la competencia técnica en vigor, conforme a la norma UNE-EN ISO/IEC 17025, cuyo alcance incluya los criterios, métodos y normas de evaluación recogidos en el Capítulo VI.

b) Cumplimiento de los requisitos de seguridad establecidos en la Sección 1.ª o en la Sección 2.ª de este Capítulo, según corresponda.

c) Desarrollo de las evaluaciones de acuerdo a procedimientos que recojan las obligaciones de información y coordinación con el Organismo de Certificación, indicadas en la Sección 3.ª de este mismo Capítulo.

2. La comprobación del cumplimiento de estos requisitos se realizará mediante el procedimiento de auditoría y seguimiento indicado en las Secciones 4.ª y 5.ª del Capítulo IV.

En todo caso, el alcance de la acreditación, otorgada por el Organismo de Certificación, estará limitado por el alcance de la acreditación de la competencia técnica del laboratorio, y cualificado por el nivel de seguridad del mismo.

3. Salvo en los casos en que haya una compartimentación organizativa, de medios y de procedimientos, aprobada por el Organismo de Certificación, el laboratorio deberá cumplir con los requisitos de gestión de seguridad, necesarios para la acreditación, incluso en el desarrollo de aquellas evaluaciones cuyo objeto final no sea la certificación del producto evaluado por parte del Organismo de Certificación.

Sección 1.ª Requisitos de seguridad para laboratorios que evalúen productos clasificados

Artículo 23. *Requisitos de laboratorios que evalúen productos clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que pretendan evaluar productos clasificados deberán cumplir, además de los requisitos establecidos para los laboratorios que evalúen productos no clasificados, lo dispuesto en la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el Manual de Protección de Materias Clasificadas del Ministerio de Defensa en poder de las empresas.

Asimismo, deberán tener suscrito, y en vigor, Acuerdo de Seguridad, con un grado de calificación de seguridad igual o superior al grado de calificación de seguridad de la información del producto a evaluar.

Sección 2.ª Requisitos de seguridad para laboratorios que evalúen productos no clasificados

Artículo 24. *Requisitos de laboratorios que evalúen productos no clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que evalúen productos no clasificados, cumplirán con los requisitos de gestión de la seguridad, aplicables a la información de las evaluaciones, establecidos en esta Sección.

Subsección 1.ª Responsabilidades del laboratorio

Artículo 25. *Derecho de acceso a la información de las evaluaciones.*

El laboratorio facilitará al Organismo de Certificación el acceso a toda la información de las evaluaciones que lleve a cabo.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de permitir a terceros, incluido el fabricante del producto evaluado, cualquier tipo de acceso a la información de las evaluaciones, tales como, planes, pruebas, análisis y resultados de la evaluación.

El Organismo de Certificación podrá prohibir la difusión de determinada información originada por el laboratorio.

Artículo 26. *Plan de protección.*

1. El laboratorio deberá elaborar, poner en práctica y mantener al día un Plan de Protección de la Información de las evaluaciones.

2. Este plan incluirá, al menos, la siguiente información:

a) Una descripción del laboratorio, con indicación expresa de la ubicación, actividades empresariales distintas a las de evaluación, en su caso, organigrama, recursos humanos, factorías, sucursales y dependencias autónomas, incluyendo un plano con leyenda de las instalaciones del laboratorio.

b) Los fundamentos del Plan, que deberán comprender los objetivos concretos que han de alcanzarse con el mismo y que estarán dirigidos a prevenir, detectar y rehabilitar el daño causado por la manifestación del riesgo, así como la identificación de los riesgos contra los que se pretende la protección.

La confidencialidad, integridad y disponibilidad de la información de las evaluaciones serán del máximo interés para el Organismo de Certificación.

c) La descripción de la organización, donde se debe documentar la estructura de seguridad del laboratorio, la matriz de responsabilidades donde se establece la identificación exacta de los responsables en lo referente a la toma de decisiones, y la definición detallada de las misiones de cada componente del sistema, así como la coordinación del apoyo potencial de organismo exteriores, tales como empresas de seguridad privada, centrales receptoras de alarmas, servicios de custodia de información, etc.

d) La descripción de las medidas de protección física, y el establecimiento de zonas de acceso restringido en las distintas dependencias del laboratorio.

e) Los Procedimientos Operativos de seguridad.

f) La descripción de las reacciones específicas a cada incidente de seguridad, desarrollando la matriz de responsabilidades en los cometidos y misiones que este plan asigne a la dirección del laboratorio, a los que formen parte del Servicio de Protección del laboratorio y al resto de personal, en lo que respecta a decisiones y actuaciones ante los riesgos de seguridad que se manifiesten y que se hayan considerado.

g) Los requisitos específicos de seguridad y los Procedimientos Operativos de seguridad de los sistemas de información del laboratorio.

Artículo 27. *Procedimientos Operativos de seguridad.*

1. Los Procedimientos Operativos de seguridad incluirán, en forma de directivas, los detalles específicos de actuación encaminados a la prevención de riesgos.

2. Estas actuaciones se deben corresponder con la matriz de responsabilidades, tratando de forma concreta y específica los siguientes aspectos, relativos a requisitos de seguridad establecidos por las condiciones de acreditación del laboratorio:

a) Las normas para el manejo y custodia de la información de las evaluaciones.

b) El tratamiento de las visitas, verificando periódicamente la eficacia del control de visitas al laboratorio, así como el correcto uso del libro de visitas o sistema alternativo.

c) La entrada en las zonas de acceso restringido.

d) El acceso, transmisión, reproducción, archivo y destrucción de información de las evaluaciones, con el establecimiento de los mecanismos necesarios que permitan identificar, en todo momento, al responsable de la tenencia de la información.

e) La regulación de las necesarias comprobaciones de seguridad, tanto durante la jornada de trabajo como al término de la misma.

f) La descripción del sistema de control de llaves.

g) El establecimiento del sistema de recibo interno, para control de información de las evaluaciones.

h) La operativa de actuación ante una incidencia de la central receptora de alarmas.

i) Los procedimientos de actuación de los vigilantes de seguridad.

Artículo 28. *Personal del laboratorio.*

El laboratorio deberá mantener actualizado un registro de seguridad de todo el personal afecto al mismo.

El laboratorio regulará, en base a la necesidad de conocer, el acceso de dicho personal a la información de las evaluaciones. Las autorizaciones de acceso a la información de las evaluaciones se comunicarán y revocarán por escrito, adjuntándose dichas comunicaciones al registro de seguridad del personal.

Artículo 29. *Comunicaciones preceptivas al Organismo de Certificación.*

El laboratorio deberá informar al Organismo de Certificación, en el plazo más breve posible, de lo siguiente:

a) Sobre toda información que llegue a su conocimiento en relación con accesos, o intentos de acceso, no autorizados a información de las evaluaciones; actos de sabotaje, o actividades que supongan un riesgo para dicha información.

b) Sobre toda anomalía, extravío, robo o manipulación relacionada con la información de las evaluaciones.

c) Sobre la presunción de que una transmisión de información de las evaluaciones haya sufrido vulneración o retraso injustificado.

d) Sobre las modificaciones que pretenda realizar en las zonas de acceso restringido.

e) Sobre las visitas que reciba conforme a lo que se expresa en la Subsección 5.ª, presente Capítulo y Sección.

f) Sobre las modificaciones del Plan de Protección, así como de las altas y bajas de personal y sobre la composición y cambios del Servicio de Protección.

Artículo 30. *Relaciones del laboratorio con contratistas.*

Los requisitos de seguridad requeridos por la acreditación del laboratorio, son también de aplicación a los contratistas del mismo que vayan a acceder a información de las evaluaciones.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de proporcionar al contratista el acceso a información de las evaluaciones. En su solicitud, comunicará los datos de identificación del contratista, así como la información de las evaluaciones a las que pudiera tener acceso, y el objeto y condiciones específicas de dicho acceso.

Como norma general, para la concesión de la autorización de acceso, el contratista deberá demostrar el cumplimiento de los requisitos de seguridad establecidos en el presente Reglamento mediante auditoría del Organismo de Certificación, conforme al procedimiento establecido en el Capítulo IV, salvo en los casos en que el Organismo de Certificación determine la aplicación de condiciones o limitaciones particulares a dicho acceso.

Subsección 2.ª Tratamiento de la información de las evaluaciones

Artículo 31. *Distintivos.*

1. Toda información de las evaluaciones llevará, de forma clara y visible, un signo distintivo de tal condición, que indicará la evaluación a la que corresponde.

2. Si se trata de documentos sueltos, se pondrá el signo distintivo en la parte superior e inferior de cada una de las páginas, centrado en las mismas, de tal forma que no pueda quedar oculto por dobleces, grapas, cubiertas, etc.

3. Si se trata de documentos permanentemente unidos o encuadernados, se pondrá el mencionado distintivo en la cubierta anterior y posterior, así como en todas sus páginas, conforme a lo indicado anteriormente.

4. Si se trata de planos, diagramas, esquemas o documentos similares, dicho distintivo se situará en la carátula y en la parte que identifique el documento.

5. Los soportes y sistemas informáticos que contengan o procesen información de las evaluaciones, se marcarán con los distintivos apropiados, para lo cual podrán emplearse etiquetas o cintas adhesivas.

6. Se seguirán procedimientos análogos para la protección de la información de las evaluaciones soportada en cualquier elemento, o conjunto de elementos, físicamente separables.

Artículo 32. *Libro registro de información de las evaluaciones.*

1. En cada dependencia del laboratorio donde se custodie información de las evaluaciones, existirá un registro donde figurará toda la información de las evaluaciones que haya tenido entrada o salida, las reproducciones y destrucciones, así como el acceso a dicha información por personal, tanto propio, como ajeno al laboratorio, con independencia de si esta información se almacena o transmite en papel o en soporte electrónico.

2. El registro se podrá mantener en soporte informático, en soporte papel (en forma de libro) o en una combinación de ambos soportes.

3. Estos registros deberán ser custodiados con la debida protección electrónica, si están en soporte informático, o en los muebles de seguridad ubicados en la zona de acceso restringido, si están en soporte papel.

4. El laboratorio deberá implementar los mecanismos correspondientes para que el registro de entrada/salida mediante soporte electrónico no se pueda eludir por el personal del mismo.

Artículo 33. *Recepción y recibo de la información de las evaluaciones.*

Cuando se reciba cualquier información de las evaluaciones, se seguirá el siguiente proceso:

a) Se examinará el envío para asegurarse de que no ha sido violado, comprobándose el contenido contra recibo. La evidencia de violación y las anomalías que se observen en el contenido deberán notificarse, cuanto antes, al remitente y al Organismo de Certificación.

b) Cuando el envío esté en orden, se firmará el recibo y se devolverá debidamente cumplimentado al remitente, realizando de manera inmediata la anotación en el libro registro.

Artículo 34. *Transmisión de la información de las evaluaciones.*

1. Se entiende por transmisión de la información de las evaluaciones, su traslado, comunicación, envío, entrega o divulgación a terceros.

2. Será necesario que la transmisión y custodia de la información de las evaluaciones sea controlada por un sistema de recibos, incluso dentro de las dependencias del laboratorio, con el fin de identificar, en cualquier momento, al responsable de su tenencia.

3. Cuando se trate de transmisión no electrónica de información de las evaluaciones, se realizará de la siguiente forma:

a) Por entrega directa del personal del laboratorio.

b) Por correo certificado nacional.

c) Por transportistas comerciales.

d) El embalaje de la información se llevará a cabo de forma que se pueda detectar su apertura; con cubiertas opacas que impidan desvelar su contenido, de tal naturaleza y resistencia, que aseguren su integridad durante el transporte; y, dicho embalaje, no tendrá ninguna indicación externa de la información contenida.

4. Cuando se trate de transmisión electrónica de información de las evaluaciones, se realizará utilizando las medidas técnicas y operacionales de protección de su confidencialidad que determine, en cada caso, el Organismo de Certificación.

Artículo 35. *Reproducción de la información de las evaluaciones.*

1. El número de reproducciones de la información de las evaluaciones, será el mínimo imprescindible. Se controlará mediante una correlativa numeración, que se recogerá en el registro, como anotación suplementaria del correspondiente original, indicando todos los datos referentes a dichas reproducciones y a la situación de cada una de ellas.

2. Cada reproducción, total o parcial, de información de las evaluaciones deberá ser numerada y tratada, a todos los efectos, como el original.

3. La reproducción de información de las evaluaciones deberá realizarse directamente por el laboratorio, sin recurrir a contratistas de artes gráficas. Se deberá comprobar, después de realizar las reproducciones, que en el mecanismo de reproducción no queda registro de la información reproducida.

Artículo 36. *Custodia y destrucción de la información de las evaluaciones.*

1. El laboratorio custodiará, por un plazo mínimo de cinco años, toda la información de cada evaluación, a contar desde la fecha de emisión del certificado correspondiente, o de la emisión del último informe técnico de evaluación, en el caso de productos no certificados.

2. En el caso de reevaluaciones, mantenimiento o extensiones del certificado, el cómputo de cinco años se referirá siempre al último certificado o informe técnico de evaluación aplicable.

3. Pasado dicho plazo, y tras obtener del Organismo de Certificación autorización escrita, procederá a su destrucción, de forma que se garantice que la información de las evaluaciones queda irreconocible y se impida su reconstrucción, total o parcial.

4. El Organismo de Certificación, previo a la autorización de destrucción, podrá requerir al laboratorio el traslado de cuanta información de las evaluaciones sea de su interés.

Artículo 37. *Inventario anual.*

El laboratorio presentará ante el Organismo de Certificación, antes del diez de enero de cada año, un inventario anual de toda la información de las evaluaciones que obran en su poder a fecha treinta y uno de diciembre del año anterior.

Subsección 3.ª Servicio de Protección de la información de las evaluaciones

Artículo 38. *Miembros del Servicio de Protección.*

1. En la organización del laboratorio, el Servicio de Protección de la información de las evaluaciones estará constituido, al menos, por el jefe del Servicio de Protección, el director del Servicio de Protección y el administrador de seguridad del sistema de información.

2. Los miembros del Servicio de Protección nombrados en el párrafo anterior son los responsables, ante el Organismo de Certificación, de la correcta aplicación de los requisitos de seguridad indicados, por ello deben contar con el adecuado grado de representatividad y autoridad, dentro de la organización del laboratorio.

3. Sus funciones de seguridad no podrán quedar disminuidas en ningún momento, aún cuando desempeñen otros cometidos en el laboratorio, debiendo contar con los medios necesarios para realizar sus funciones con eficacia.

Artículo 39. *Condiciones personales y nombramiento.*

1. Los responsables del Servicio de Protección deberán tener dependencia directa de la dirección del laboratorio, una relación laboral estable sobre la base de continuidad en su función y se les reconocerá, dentro del laboratorio, la debida autoridad en el desempeño de sus cometidos.

Deberán gozar de prestigio personal y profesional, y tener un amplio conocimiento de la organización del laboratorio.

2. El nombramiento y cese de los responsables del Servicio de Protección se comunicará por escrito, reconocido expresamente, en el que constarán las misiones de la responsabilidad asignada.

3. La inadecuación en el desarrollo, o la inobservancia, de las misiones encomendadas a los responsables del Servicio de Protección, podrá motivar su cese, cuando el Organismo de Certificación así lo demande, previa notificación por escrito, y sin perjuicio de la exigencia de otras responsabilidades que se pudieran derivar.

Artículo 40. *Director del Servicio de Protección.*

1. Cuando el laboratorio designe varios jefes del Servicio de Protección de la información de las evaluaciones, uno por cada una de las sedes donde se maneje o custodie información de las evaluaciones, deberá nombrar un director del Servicio de Protección, cuya misión principal será coordinar la actuación de dichos jefes, así como de los distintos administradores de seguridad del sistema de información, sin que esto suponga merma alguna de las responsabilidades que a éstos corresponde.

2. El cargo de director del Servicio de Protección se podrá compatibilizar con el de jefe de dicho Servicio, en las dependencias donde se ubiquen las oficinas centrales del laboratorio.

Artículo 41. *Misiones del jefe del Servicio de Protección.*

1. Corresponde al jefe del Servicio de Protección la misión de organizar, dirigir y controlar el sistema de protección para salvaguarda de la información de las evaluaciones, y la obligación de cumplir y hacer cumplir, en todas sus partes, estos requisitos de seguridad para la acreditación del laboratorio.

2. Entre los cometidos del jefe del Servicio de Protección se encuentran:

a) Asegurar la protección de la información de las evaluaciones en poder del laboratorio.

b) Regular el acceso a la información de las evaluaciones conforme a los criterios y procedimientos establecidos.

c) Llevar a cabo un programa de formación del personal del laboratorio, con una periodicidad mínima de treinta (30) meses, cuyo principal objetivo será sensibilizar a dicho personal sobre la importancia de cumplir los procedimientos de protección de la información de las evaluaciones y el deber de discreción.

d) Controlar la recepción, custodia, reproducción, destrucción y devolución de la información de las evaluaciones, conforme a los procedimientos establecidos.

e) Velar, especialmente, para que ninguna información de las evaluaciones sea transmitida indebidamente, o sea manejada o custodiada en lugar distinto a las zonas protegidas.

f) Elaborar, implantar y mantener el Plan de Protección conforme a lo establecido en este Reglamento.

g) Mantener actualizados los registros de seguridad.

Artículo 42. *Misión del administrador de seguridad del sistema de información.*

1. El administrador de seguridad del sistema de información tendrá como misión organizar, dirigir y controlar la seguridad del sistema de información del laboratorio. Este administrador podrá ser el propio jefe del Servicio de Protección, cuando tenga la formación adecuada.

2. Entre los cometidos del administrador de seguridad del sistema de información se encuentran:

a) Elaborar, organizar e implementar los requisitos y procedimientos relativos a la seguridad de los sistemas de información del laboratorio, debiendo revisar, periódicamente, la eficacia de todos los componentes.

b) Controlar que todo el personal que tiene acceso al sistema de información está debidamente autorizado.

c) Investigar los incidentes de seguridad que pudieran afectar al sistema de información, evaluando en su caso, los daños causados e informando de las conclusiones al jefe del Servicio de Protección.

d) Llevar a cabo un programa de formación continua de los usuarios del sistema de información, sobre la observancia de los procedimientos de seguridad.

e) Gestionar y proporcionar los códigos de acceso u otros dispositivos de control de acceso al sistema de información. Llevará un registro de asignación de códigos a los usuarios, que serán cambiados con una periodicidad mínima de tres meses, y cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa dichos códigos.

f) Realizar la gestión de claves del sistema de información del laboratorio, incluidos los sistemas de cifra que estuvieran en el ámbito de su competencia, así como la de los sistemas de soporte a la evaluación. Para ello, controlará su generación, almacenamiento, distribución, expiración y destrucción. En la recepción de nuevos equipos modificará todas las claves que, por defecto, vengan de fábrica.

g) Controlar tanto las modificaciones que se realicen en cualquier componente del sistema de información, asegurándose que no se vea afectada la seguridad del sistema, como los aspectos de la gestión de la configuración de dichas modificaciones.

h) Comprobar que el mantenimiento del sistema de información se realiza conforme a los procedimientos y requisitos operativos de seguridad.

i) Verificar que los soportes de almacenamiento que incluyan información de las evaluaciones se custodian debidamente.

j) Evaluar los registros de seguridad del sistema de información, asegurándose que son suficientes para llevar a cabo un control eficaz. Deberán incluir aquellas actividades, con indicación del usuario, hora y fecha, en que se produzcan hechos que puedan afectar a la seguridad del sistema, como finalizaciones anormales del trabajo, cierres indebidos del sistema, fallos en los mecanismos de seguridad, intentos no autorizados de acceso a datos

de la evaluación, uso del sistema de un modo no autorizado, copias e impresiones de la información de las evaluaciones, etc.

k) Controlar y registrar las copias periódicas de seguridad.

Subsección 4.ª Inspecciones de seguridad

Artículo 43. *Inspectores de seguridad.*

Los inspectores de seguridad son los representantes del Organismo de Certificación, ante el laboratorio, para la comprobación de la correcta aplicación de los requisitos de seguridad exigidos en el proceso de acreditación.

El laboratorio les reconocerá las competencias que les atribuyen estos requisitos, asumiendo el compromiso de facilitarles su labor, y dispondrá los medios precisos para que realicen sus funciones con eficacia.

Artículo 44. *Nombramiento.*

El Organismo de Certificación notificará al laboratorio la identidad del inspector de seguridad correspondiente, así como los cambios que se produzcan.

El nombramiento de inspector de seguridad, para un mismo laboratorio, podrá recaer en varias personas, si el Organismo de Certificación así lo estima oportuno.

Artículo 45. *Misiones del inspector de seguridad.*

Corresponde al inspector de seguridad:

a) La observancia del exacto cumplimiento de las obligaciones y compromisos que contrae el laboratorio en el proceso de acreditación.

b) Asesorar al laboratorio en la puesta en práctica de los procedimientos de seguridad, que garanticen la protección de la información de las evaluaciones.

Artículo 46. *Inspecciones.*

1. La inspección constituye uno de los medios por los que el Organismo de Certificación comprueba el cumplimiento, por parte del laboratorio, de los requisitos de seguridad para la acreditación.

2. Las inspecciones serán ordinarias cuando se realizan de forma periódica, por los inspectores de seguridad nombrados específicamente para cada laboratorio. Las inspecciones ordinarias no precisan concertación previa.

3. Las inspecciones extraordinarias se realizarán cuando el Organismo de Certificación lo estime conveniente, y serán llevadas a cabo por las personas que éste designe. Las inspecciones extraordinarias se comunicarán previamente al laboratorio.

4. En las inspecciones estarán obligados a estar presentes, el jefe del Servicio de Protección, o quien le sustituya, debidamente acreditado en el caso justificado de que el primero no pudiera asistir, y el personal dependiente del laboratorio que designe el Organismo de Certificación.

5. El inspector de seguridad, en las inspecciones ordinarias, o el jefe de la comisión del Organismo de Certificación, en las inspecciones extraordinarias, deberá anotar en el registro del laboratorio, un resumen del resultado de la inspección. En el caso de presentar aspectos negativos, se remitirá al laboratorio la correspondiente comunicación, en la que se deberá reflejar el plazo de corrección para solventar las anomalías observadas por la inspección.

Subsección 5.ª Visitas

Artículo 47. *Consideración de visita.*

Se considera visita, el acceso físico y circunstancial de una o varias personas, sin relación de dependencia directa con el laboratorio, a las dependencias o instalaciones del mismo.

Artículo 48. *Registro de visitas.*

Las visitas se anotarán en el registro de visitas, antes de efectuar la visita. Se deberán recoger, como mínimo, los siguientes datos: fecha de la visita, nombre completo del visitante, número del DNI o pasaporte, nacionalidad, empresa/organismo o dirección del visitante, y nombre de la persona visitada.

Este registro estará a disposición del Organismo de Certificación, para su consulta.

Artículo 49. *Normas para el control de visitas.*

Para el control de las visitas, se seguirán las siguiente normas:

a) El laboratorio controlará el movimiento de las visitas que entren en sus dependencias, para garantizar la debida seguridad de la información de las evaluaciones que custodie.

b) Se prohibirá al visitante efectuar cualquier tipo de registro o reproducción de la información de las evaluaciones, que deberá solicitarse al personal del laboratorio y ser efectuado mediante los procedimientos correspondientes.

c) Toda entrega al visitante de información de las evaluaciones será anotada en el registro.

Artículo 50. *Visitas de larga duración.*

Tendrán consideración de visitas de larga duración, las realizadas sobre la base de continuidad o reiteración, por un periodo de doce meses. Tales visitas se anotarán en el registro de seguridad de personal, incluyendo las autorizaciones de acceso a la información de evaluaciones que se pudieran conceder.

Subsección 6.ª Zonas de acceso restringido

Artículo 51. *Sistema de protección.*

1. El laboratorio implantará un sistema de protección, integrado en la estructura empresarial, que permita proteger la información de las evaluaciones contra los riesgos que puedan implicar una amenaza para la misma.

2. El sistema de protección puede entenderse como el conjunto de recursos y procedimientos que, interactuando coordinadamente, tienen como finalidad proteger la información de las evaluaciones de los riesgos que puedan afectar a su integridad, confidencialidad o disponibilidad.

Artículo 52. *Características del sistema de protección.*

El documento donde se definen las características que presenta el sistema de protección es el Plan de Protección, definido en el Artículo 26.

El laboratorio deberá adjuntar, al Plan de Protección, un proyecto del subsistema de protección física, que estará compuesto por una memoria justificativa de los criterios de diseño, la descripción detallada de todos los componentes de la instalación y los planos que especifiquen la ubicación física de los mencionados componentes.

Artículo 53. *Subsistema de protección física.*

El subsistema de protección física, que ha de instalarse, obligatoriamente, en las dependencias del laboratorio donde se vaya a manejar información de las evaluaciones, ha de mantenerse en un óptimo grado de eficacia y utilidad para el cumplimiento de las condiciones de acreditación del laboratorio. La valoración de dicha eficacia y utilidad corresponde al Organismo de Certificación.

Las áreas de acceso restringido, que deberá considerar el subsistema de protección física, están compuestas por las zonas de evaluación y las zonas de protección.

Artículo 54. *Zonas de evaluación.*

Las zonas de evaluación son las constituidas por aquellas dependencias del laboratorio en las que, únicamente, se debe manejar y custodiar información de las evaluaciones, con las siguientes características:

a) Ha de estar construida de forma que quede limitado, materialmente, el acceso a la misma, y de manera que se pueda apreciar, con una simple inspección, una intrusión a través de las paredes, suelo, puertas o ventanas que delimiten la zona. Estos elementos no deben permitir la observación desde el exterior.

b) Las puertas de acceso deben disponer de una cerradura de bloque con llave, cuyo mecanismo será obligatoriamente accionado, cuando en el interior se esté trabajando con información de las evaluaciones, así como cuando no haya nadie en la misma. También dispondrán de un dispositivo que obligue a la puerta a permanecer cerrada, cuando no se esté franqueando, y dispondrán de detector de apertura.

c) Si se incluyen ventanas, deben colocarse dispositivos que detecten su apertura, en el caso de ser practicables, así como detectores de rotura de cristales. Los elementos translúcidos deberán estar acondicionados para impedir la observación desde el exterior. En el caso de que las ventanas tengan fácil acceso desde el exterior, estarán físicamente protegidas.

d) Se implantarán medidas físicas y organizativas para impedir el acceso a la zona de evaluación, al personal que no tenga derecho de acceso a la información de las evaluaciones y, en el caso en que se divida esta zona por evaluaciones, al personal que no tenga derecho de acceso, en particular, a la información de la evaluación asociada a cada división.

e) Deberá contar con una caja fuerte Nivel IV, conforme a la norma UNE-EN 1143-1-98, equipada con cerradura Clase B, según norma EN 1300, donde se custodiará, obligatoriamente, la información de las evaluaciones durante los períodos de tiempo en que no se esté manejando. Deberá reunir, además, las características siguientes:

Si se trata de caja fuerte autónoma, ha de estar anclada si su volumen es inferior a 500 litros, o si su peso no supera los 1.000 Kg.

Si se trata de caja fuerte empotrada, el grado de seguridad del alojamiento donde se ubique ésta ha de proporcionar, como mínimo, el atribuido al de la puerta y marco de la caja.

Doble sistema de apertura, uno de los cuales ha de ser, ineludiblemente, de combinación electrónica.

Artículo 55. *Zonas de protección.*

Las zonas de protección son las constituidas por el entorno de las zonas de evaluación en el que no se podrá manejar o custodiar información de las evaluaciones, pero que estarán dotadas de medidas de seguridad, con la finalidad de incrementar la seguridad de las zonas de evaluación y tendrán las siguientes características:

a) Su ubicación dependerá de las características constructivas y de la situación de la zona de evaluación.

b) En cualquier caso, se implementarán las medidas físicas y organizativas suficientes para que el personal que acceda a la zona de protección esté identificado.

Artículo 56. *Central de alarmas.*

Además de los requisitos establecidos en los artículos 54 y 55, las zonas de evaluación y de protección dispondrán de las siguientes medidas de seguridad:

a) Todos los medios activos de seguridad deben estar conectados físicamente a un centro de control de alarmas, que disponga de una autonomía mínima de setenta y dos horas, provista de un dispositivo antisabotaje y ubicada de manera oculta.

b) Este centro de control quedará activado, obligatoriamente, fuera del horario laboral y estará conectado con una central receptora de alarmas, que pueda gestionar cualquier alarma de forma oportuna.

c) La conexión con la central receptora de alarmas debe permitir la verificación automática de la línea de comunicación, para poder conocer oportunamente una interrupción en la misma, a través de la correspondiente señal de alarma. La operativa de la gestión de la central receptora de alarmas deberá estar incluida en el Plan de Protección.

d) Los códigos de acceso de la central de alarmas, que permiten su programación y control, deberán ser conocidos, únicamente, por el jefe del Servicio de Protección y las personas por él designadas. Dicha designación quedará anotada en el registro de seguridad del personal. Los códigos deberán modificarse con los criterios indicados en el artículo 57, referido a «Combinaciones, códigos de acceso y control de llaves», que sigue.

Subsección 7.ª Procedimiento de seguridad

Artículo 57. *Combinaciones, códigos de acceso y control de llaves.*

1. Sólo tendrán conocimiento de los códigos de acceso a las zonas de evaluación, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de custodia de la información de las evaluaciones, el jefe del Servicio de Protección y las personas que él designe, que serán las mínimas imprescindibles.

2. Las llaves de las cajas fuertes no podrán salir de la sede del laboratorio bajo ningún concepto, debiendo guardarse de forma oculta y segura, y en distinto lugar al que se custodien las claves de combinación para la apertura de las mismas.

3. Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes a las que se refieren.

4. Las claves de combinación para la apertura de las cajas fuertes y los códigos de control de la central de alarmas no deben conservarse en claro, sino de manera cifrada, debiendo ser modificados, obligatoriamente, en los siguientes casos:

a) Al recibirse los muebles de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.

b) Cada seis meses.

c) Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas, incluido el personal de las empresas de mantenimiento.

d) Cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa las claves o los códigos.

Artículo 58. *Acceso físico a la información de las evaluaciones.*

Cuando se precise el acceso físico a la información de las evaluaciones, el jefe del Servicio de Protección de la información, o persona designada por él, pondrá dicha información a disposición de los empleados del laboratorio que cuenten con las debidas autorizaciones de acceso a la misma, la cual deberá ser manejada exclusivamente en la zona de evaluación, estando bajo la responsabilidad de estas personas su custodia y control.

Una vez finalizado el manejo, se devolverá inmediatamente a la persona que hizo entrega de la misma, siendo almacenada en su lugar de custodia, donde permanecerá obligatoriamente.

Artículo 59. *Dispositivos técnicos de identificación.*

Siempre que el laboratorio lo considere necesario, podrá emplear dispositivos personales que faciliten y controlen el acceso, por su personal, a las zonas de acceso restringido. Los dispositivos serán diseñados de forma que se impida su empleo no autorizado, por lo que, cada uno de ellos se asignará a un empleado determinado, con su correspondiente código personalizado, que será conocido únicamente por el interesado.

De estos dispositivos no podrán determinarse las evaluaciones a cuya información tiene acceso el empleado al que se le asigna.

En su caso, deberá notificarse al Organismo de Certificación el sistema adoptado, debiéndose plasmar la operativa del mismo en el Plan de Protección.

Subsección 8.ª Seguridad de los sistemas de información

Artículo 60. *Seguridad de la información sobre evaluaciones.*

1. La información de las evaluaciones es un bien que debe ser protegido de manera que se garantice su confidencialidad, su integridad y disponibilidad, a lo largo de toda su existencia, con independencia del medio, soporte o formato en el que permanezca o se transmita. Para ello, también es necesario asegurar la integridad y disponibilidad de los servicios y recursos que sustentan dicha información.

2. Los mecanismos de seguridad del sistema de información que procese, almacene o transmita información de las evaluaciones, tienen como finalidad evitar accesos, destrucciones y modificaciones no permitidas, asegurando, al mismo tiempo, que la información es utilizada cuándo y cómo lo requieran los usuarios autorizados.

3. Los factores que se han de evaluar en la protección de la información de las evaluaciones serán los siguientes:

a) Confidencialidad, como servicio de seguridad que pretende que una información sea revelada exclusivamente a los usuarios, entidades o procesos autorizados.

b) Integridad, como medida que asegura que la información sea creada, modificada o borrada sólo por personas, entidades o procesos autorizados.

c) Disponibilidad, para que la información sea utilizable en el lugar, momento y forma que lo requieran lo usuarios, entidades o procesos autorizados.

4. El laboratorio deberá concretar los principios y reglas básicas de seguridad, exigidos para la acreditación, en unos procedimientos específicos para la protección de la información de las evaluaciones tratadas en su sistema de información, cuya seguridad deberá estar necesariamente integrada en el sistema de protección del laboratorio.

5. La seguridad del sistema de información requiere la adecuada aplicación de procedimientos y normas que posibiliten el control de acceso al sistema, la distribución de responsabilidades, la segregación de funciones y la compartimentación de los entornos correspondientes a las evaluaciones y a la administración y gestión del laboratorio.

Artículo 61. *Usuario del sistema de información.*

1. El usuario del sistema de información que maneje información de las evaluaciones dependerá directamente, en todo lo referente a la seguridad del sistema, del administrador de seguridad del sistema de información, al que informará inmediatamente del menor indicio o conocimiento de cualquier hecho que afecte a la seguridad de la información de las evaluaciones.

2. La responsabilidad de cada usuario es básica para la seguridad del sistema. Por ello es imprescindible la autenticación del usuario. Se entenderá por autenticación el proceso que confirma su identidad.

Bajo ningún concepto este usuario podrá emplear equipos y medios particulares para el tratamiento de la información de las evaluaciones.

El usuario se asegurará que su código personal no es utilizado por otra persona, recomendándose la memorización del mismo, sin dejar constancia escrita o, en su caso, guardando el registro de forma oculta y segura; no hacer uso del código cuando se está siendo observado y no compartir, en ningún caso, el código personal con otros usuarios del sistema.

3. En los sistemas que lo permitan, el usuario realizará copias periódicas de seguridad de la información de las evaluaciones, bajo la supervisión del administrador de seguridad del sistema de información, quien llevará el control y registro oportuno.

Artículo 62. *Soportes de almacenamiento de información de las evaluaciones.*

1. Los soportes removibles reutilizables, que hayan contenido información de las evaluaciones, podrán volverse a emplear una vez que se haya efectuado el borrado seguro mediante procedimientos que garanticen el mismo.

Esto también se aplicará a los soportes fijos de los equipos utilizados en las pruebas de evaluación, así como en los destinados a la instalación, o recreación, del producto a evaluar y a su entorno de pruebas, que deberán borrarse de manera segura al término de cada evaluación.

El resto de soportes fijos de información del laboratorio deberán ser tratados según procedimientos específicos, que serán reseñados en los Procedimientos Operativos de seguridad, de forma que se imposibilite la extracción de información por personal no autorizado.

2. Toda información que tenga entrada mediante comunicaciones electrónicas, o soporte removible, deberá ser comprobada en un sistema aislado, previamente a su inclusión en el sistema de información del laboratorio, a fin de detectar la posible presencia de elementos extraños, dañinos o de mal funcionamiento. Dicha comprobación, y su resultado, quedarán anotados en el libro registro del laboratorio junto con la anotación de la entrada de la información.

Artículo 63. *Características físicas de las instalaciones.*

1. El sistema de información que se utilice para el tratamiento de la información de las evaluaciones deberá estar situado en la zona de evaluación y, obligatoriamente, ubicado en territorio nacional.

2. Los equipos periféricos de impresión de documentos estarán insonorizados, cuando las características de los mismos lo requieran, y así lo determine el Organismo de Certificación.

3. No se podrá realizar ningún cambio en la ubicación física de los elementos del sistema de información, sin el control del administrador de seguridad, y la aprobación del jefe del Servicio de Protección de la información de las evaluaciones.

Artículo 64. *Procedimientos operativos de seguridad.*

1. El administrador de seguridad del sistema de información del laboratorio elaborará unos Procedimientos Operativos de seguridad, donde se describirán, detalladamente, las operaciones necesarias para proteger dicho sistema.

2. Estos procedimientos operativos de seguridad han de cumplir los requisitos de seguridad para la acreditación del laboratorio, incluirse en el Plan de Protección y, adicionalmente, contemplarán lo siguiente:

a) La revisión bianual del grado de cumplimiento de la eficacia de los propios procedimientos operativos, y del cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

b) La aplicación de medidas de protección contra elementos dañinos o maliciosos (virus, caballos de Troya, gusanos, etc.).

c) El cambio trimestral de los códigos de acceso de los usuarios.

d) La aplicación de un sistema de borrado rápido o destrucción de la información de las evaluaciones, para casos de emergencia.

e) La utilización de un sistema de alimentación ininterrumpida, de duración suficiente, para salvaguardar los procesos en curso.

Artículo 65. *Interconexión de sistemas.*

1. Como norma general, el sistema de información donde se trate información de las evaluaciones, deberá estar aislado.

Excepcionalmente pueden existir situaciones en las que el sistema necesite estar interconectado con otros, bien para comunicar varias zonas de evaluación del laboratorio, separadas físicamente, en las que se realice la misma evaluación, o para permitir la comunicación en situaciones de naturaleza análoga.

En estas situaciones, la interconexión deberá ser autorizada por el Organismo de Certificación, que determinará los requisitos de seguridad que se deben implantar.

2. El acceso del laboratorio a redes públicas, para la consulta y descarga de información de vulnerabilidades, programas de uso en las evaluaciones y demás información relevante a las evaluaciones, no se podrá realizar en las áreas de evaluación o de protección, debiendo

tramitarse la incorporación de esta información al sistema de información del laboratorio, conforme a lo requerido en el artículo 32, «Libro registro de información de las evaluaciones».

Sección 3.ª Requisitos de los procedimientos de evaluación

Artículo 66. *Reconocimiento de actuaciones del laboratorio de evaluación.*

La certificación de la seguridad de un producto se inicia a instancias del solicitante ante el Organismo de Certificación, lo cual no obsta para que, independientemente, se puedan solicitar, por parte del mismo interesado, trabajos de evaluación equivalentes a los que requiere el Organismo de Certificación para la certificación de dicho producto.

En cualquier caso, el Organismo de Certificación únicamente reconocerá las actuaciones del laboratorio de evaluación que se realicen, completamente, bajo su conocimiento y seguimiento, conforme al procedimiento establecido en el Capítulo V del presente Reglamento.

Artículo 67. *Procedimientos de evaluación.*

Los procedimientos de evaluación del laboratorio que solicite la acreditación, deberán contemplar las obligaciones de coordinación e información con el Organismo de Certificación, indicadas en esta Sección.

Igualmente, y para la defensa de la validez y reconocimiento mutuo de certificados de la seguridad de los productos, el Organismo de Certificación trasladará al laboratorio las obligaciones requeridas, tanto al procedimiento de evaluación, como a los propios laboratorios de evaluación, en los acuerdos, convenios o contratos de reconocimiento mutuo en los que el solicitante de la certificación del producto quiera hacer valer la misma y el Organismo de Certificación opere.

Artículo 68. *Obligaciones de coordinación e información.*

El laboratorio deberá cumplir, en el desarrollo de sus trabajos de evaluación, con los requisitos de coordinación e información con el Organismo de Certificación que se incluyen en esta Sección.

Artículo 69. *Aprobación previa.*

1. El laboratorio de evaluación estará obligado a obtener aprobación previa, y por escrito, del Organismo de Certificación para comenzar los trabajos de evaluación.

En la aprobación previa deberá constar la asignación del responsable de la certificación del producto, por parte del Organismo de Certificación, a quien se dirigirán las comunicaciones relativas a la evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

2. Dicha aprobación se solicitará por el laboratorio mediante escrito, al que se acompañará lo siguiente:

a) Plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) Copia del contrato, o documento similar, que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos para la acreditación del laboratorio.

Artículo 70. *Inicio y fin de los trabajos de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, el comienzo y término de cada fase, actividad, acción y unidad de trabajo de la evaluación, según se definan en la metodología y procedimientos de evaluación a aplicar. En función de

su relevancia, el Organismo de Certificación podrá rebajar este requisito a la comunicación de fases, actividades o hitos señalados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 71. *Desviaciones del plan de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, las desviaciones con respecto al plan de evaluación, con análisis de las causas de la desviación, las medidas correctivas aplicadas por el laboratorio, y el nuevo plan de evaluación actualizado.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 72. *Dificultades en la evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, cualquier dificultad surgida en la aplicación o interpretación de las normas utilizadas, así como cualquier dificultad que condicione el normal transcurso de una evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 73. *Informes de observación.*

El laboratorio estará obligado a remitir, al Organismo de Certificación, todos los informes de observación y de disconformidad emitidos e informará de su cierre, cuando ocurra, y de las medidas correctivas aplicadas por el solicitante de la certificación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 74. *Información técnica adicional.*

El laboratorio de evaluación estará obligado a facilitar toda información técnica adicional que sea necesaria para el análisis, por parte del Organismo de Certificación, de la información de las evaluaciones, incluyendo acceso y formación sobre programas y sistemas de evaluación, elaborados o adquiridos por el laboratorio, así como aquellos métodos y técnicas de análisis de vulnerabilidades empleados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 75. *Reuniones entre el solicitante y el laboratorio.*

El laboratorio de evaluación estará obligado a comunicar, e invitar a su asistencia, al Organismo de Certificación, de cuantas reuniones celebre dicho laboratorio con el solicitante de la certificación, con indicación de su naturaleza y objeto.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 76. *Reuniones de seguimiento.*

El laboratorio de evaluación estará obligado a atender cuantas reuniones de seguimiento convoque el Organismo de Certificación. Dichas reuniones se convocarán por el responsable de la certificación del producto del Organismo de Certificación, y serán atendidas por el personal requerido para explicar e interpretar la información de las evaluaciones objeto de seguimiento. En el caso de información de las evaluaciones elaborada por el laboratorio, se podrá requerir la asistencia a la reunión de los autores de la misma.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 77. *Puesta a disposición de dependencias y sistemas.*

El laboratorio de evaluación estará obligado a poner sus dependencias y sistemas de evaluación a disposición del Organismo de Certificación, para la realización, por parte del personal del mismo, de las tareas de verificación de la actividad de evaluación que se consideren oportunas.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

CAPÍTULO IV

Acreditación de laboratorios

Sección 1.ª Acreditación

Artículo 78. *Acreditación.*

El Organismo de Certificación acreditará a los laboratorios solicitantes siguiendo el procedimiento establecido en la Sección 4.ª de este Capítulo y en base al cumplimiento de los requisitos establecidos en el Capítulo III.

Artículo 79. *Solicitantes.*

Pueden solicitar esta acreditación cualesquiera laboratorios de evaluación de la seguridad de los sistemas de información, con independencia de su naturaleza jurídica, pública o privada, sin más limitación que la de realizar su actividad de evaluación en territorio español.

Artículo 80. *Contenido de la acreditación.*

La acreditación de un laboratorio supone el reconocimiento de su competencia técnica, de la adecuación de la gestión de la seguridad del mismo a las particularidades de la evaluación de la seguridad de las Tecnologías de la Información, y de la consideración de los requisitos de coordinación e información al Organismo de Certificación, que permitirá a éste basar su dictamen de certificación de un producto, entre otros factores, en el informe de evaluación del laboratorio acreditado.

La acreditación de un laboratorio no presupone, sin embargo, aceptación incondicional de los resultados de la actuación de evaluación de un producto determinado. Dicha aceptación se otorgará tras el análisis inicial de la solicitud de certificación, mediante el seguimiento de la labor de evaluación y tras el análisis del correspondiente informe técnico de evaluación, tal y como se define en el Capítulo V.

Artículo 81. *Duración de la acreditación.*

La acreditación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme se regula en este Capítulo.

Sección 2.ª Alcance de la acreditación

Artículo 82. *Alcance de la acreditación.*

La acreditación se cualifica mediante el alcance, que limitará el reconocimiento de las actuaciones del laboratorio con relación al nivel de calificación de seguridad y con relación a las normas y niveles de evaluación.

Artículo 83. *Alcance con relación al nivel de calificación de seguridad.*

Con relación al nivel de calificación de seguridad se distinguen aquellos laboratorios con capacidad para manejar información y productos clasificados, de aquellos otros que operan en el régimen de la información y productos no clasificados.

Artículo 84. *Alcance con relación a las normas y niveles de evaluación.*

La certificación de la seguridad de los productos y sistemas de las Tecnologías de la Información puede requerir la evaluación de los mismos atendiendo a diferentes criterios, métodos y normas de evaluación.

Adicionalmente, dichas normas pueden distinguir niveles de evaluación y niveles de seguridad.

El Organismo de Certificación mantiene una relación actualizada de normas aplicables, según se establece en el Capítulo VI.

El laboratorio solicitante deberá indicar, en el alcance de la acreditación, aquellas normas y niveles, de la mencionada relación, en las que demuestra competencia técnica y experiencia acreditada.

Sección 3.ª Criterios de acreditación

Artículo 85. *Criterios generales.*

1. La competencia técnica del laboratorio solicitante se determinará, en primera instancia, por la correspondiente acreditación de esta competencia, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria, y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025.

2. La acreditación de competencia técnica, que deberá ser concedida por una entidad de acreditación reconocida, ha de incluir, en su alcance, las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información, aprobados por el Organismo de Certificación, y demás limitaciones requeridas por éste.

En particular, se reconocen las acreditaciones de competencia técnica emitidas por la Entidad Nacional de Acreditación, sin perjuicio de las acreditaciones emitidas por otras entidades de acreditación que satisfagan los requisitos establecidos en el Capítulo II del Reglamento de la Infraestructura para la Calidad y Seguridad Industrial.

3. Los requisitos adicionales, de gestión de la seguridad de la información de las evaluaciones, así como los de coordinación e información al Organismo de Certificación, se incluyen en el Capítulo III.

Los requisitos indicados en el párrafo anterior, se verificarán mediante la aplicación del procedimiento establecido en la siguiente Sección, sobre la base de una auditoría del laboratorio solicitante, que incluye el seguimiento de una evaluación de prueba bajo los procedimientos y requisitos del Organismo de Certificación.

Artículo 86. *Criterios complementarios.*

Para aquellos casos que lo requieran, los criterios generales mencionados podrán ser completados o precisados por otros complementarios de carácter técnico, específicos para cada tipo de producto a evaluar, criterios, métodos y normas de evaluación de cada acreditación, o modificación del alcance de la solicitada, recogidos y publicados en los correspondientes documentos del Organismo de Certificación.

Sección 4.ª Procedimiento de acreditación

Artículo 87. *Proceso de acreditación.*

Aquellos laboratorios que deseen ser acreditados por el Organismo de Certificación, deberán someterse al proceso de acreditación establecido en la presente Sección.

Artículo 88. *Solicitud de acreditación.*

La solicitud de acreditación deberá remitirse al Director del Organismo de Certificación adjuntando, como mínimo, la siguiente información, debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.
b) Nombre del responsable del laboratorio y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evaluaciones para las que el laboratorio solicita ser acreditado.
c) Compromiso de cumplir los requisitos de acreditación del Organismo de Certificación, indicados en el Capítulo III, así como declaración de disponibilidad para la realización de la auditoría y actividades derivadas del proceso de acreditación.
d) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de evaluación de la seguridad de los productos y sistemas de las Tecnologías de la Información.
e) Alcance de la acreditación solicitada, indicando el nivel de calificación de seguridad y las normas y niveles de evaluación.
f) Relación y copia de los documentos del sistema de gestión de la calidad del laboratorio.
g) Relación y copia de los documentos del sistema de gestión de la seguridad del laboratorio.
h) Relación y copia de los manuales y procedimientos de evaluación del laboratorio.
i) Certificado de acreditación de la competencia técnica emitido por ENAC, o entidad de acreditación reconocida, según lo indicado en el artículo 85 o, en su caso, certificado de haber iniciado dicho proceso de acreditación con la entidad correspondiente.
j) Justificante del pago de las tasas de acreditación vigentes.
k) Alcance y descripción de las evaluaciones de prueba que el solicitante pretende llevar a cabo, bajo las condiciones y procedimientos de este esquema, para la demostración del cumplimiento de los requisitos de acreditación, y que han de ser de alcance igual, o superior, al de la acreditación solicitada.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 89. *Modelo de solicitud de acreditación.*

Las solicitudes de acreditación de laboratorio se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 90. *Subsanación y mejora de la solicitud de acreditación.*

A la recepción de la solicitud de acreditación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

En caso de ser necesaria la subsanación o mejora de la solicitud de acreditación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Se admitirá durante la instrucción de la solicitud de acreditación la equivalencia del certificado de acreditación de la competencia técnica por certificado de encontrarse incurso en el proceso de acreditación de dicha competencia, siendo requisito definitivo para la

acreditación del laboratorio, la certificación de su competencia técnica conforme a lo indicado en el artículo 85.

Artículo 91. *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de acreditación, incluyendo en dicha notificación:

a) El nombre y datos de contacto del responsable del procedimiento de acreditación, que será igualmente responsable de la dirección de la auditoría inicial del cumplimiento de los requisitos para la acreditación.
b) La fecha propuesta de comienzo de la auditoría indicada.

Artículo 92. *Preparación de la auditoría.*

Los técnicos designados por el Organismo de Certificación, con carácter previo a la auditoría, realizarán un estudio preliminar de la documentación recibida junto con la solicitud, relativa a los sistemas de calidad, seguridad y evaluación del laboratorio solicitante.

Las conclusiones de dicho estudio, en términos de observaciones sobre el cumplimiento e identificación de disconformidades de los requisitos para la acreditación, se remitirán al solicitante con una antelación no inferior a un mes de la fecha de comienzo de la auditoría. Junto a dichas conclusiones, y a la vista del estudio realizado, el Organismo de Certificación indicará la duración estimada de la auditoría, cuyo calendario definitivo se acordará en la fecha de comienzo de la misma.

El laboratorio solicitante podrá subsanar y mejorar la solicitud de acreditación en base a las conclusiones del estudio preliminar, con carácter previo a la realización de la auditoría.

Artículo 93. *Instrucción de la auditoría.*

La instrucción de la auditoría se realizará en tres fases: reunión inicial, desarrollo de la auditoría y reunión final.

a) Reunión inicial. En la fecha indicada por el Organismo de Certificación, se celebrará la reunión inicial de auditoría entre los representantes del laboratorio solicitante y el equipo auditor, designado por el Organismo de Certificación. En esta reunión se harán las presentaciones oportunas, se confirmará el plan y calendario de la auditoría y se revisarán las conclusiones del estudio preliminar de la solicitud.
b) Desarrollo de la auditoría. Durante esta fase se procederá a la observación del laboratorio solicitante durante la evaluación de prueba, y a la investigación del cumplimiento de los requisitos para la acreditación.
c) Reunión final. El equipo auditor se reunirá con los representantes de la entidad solicitante, con objeto de presentar un informe verbal de los resultados del desarrollo de la auditoría.

Artículo 94. *Informe del equipo auditor.*

El equipo auditor, en un plazo no superior a diez días contados desde la fecha de la reunión final de la auditoría, elaborará un informe con los resultados y con la información recopilada durante el desarrollo de la misma. Este informe será remitido al laboratorio solicitante para su conocimiento.

Artículo 95. *Audiencia previa.*

1. Una vez instruido el procedimiento de auditoría, se le pondrá de manifiesto al laboratorio solicitante y se le convocará a una reunión de audiencia previa a la resolución.
2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades identificadas durante el procedimiento de auditoría, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de acreditación.
3. El laboratorio solicitante, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el laboratorio manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

Artículo 96. *Resolución de la solicitud de acreditación.*

1. La resolución de la solicitud de acreditación se dictará de acuerdo con lo indicado en este artículo y en los plazos establecidos en el artículo 107, «Plazos y actos presuntos».

2. Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

3. La resolución de desestimación será motivada. La resolución de acreditación contendrá adicionalmente los siguientes extremos:

a) Alcance de la acreditación concedida.

b) La fecha en vigor de la acreditación y referencia a su vigencia.

Artículo 97. *Vigencia de la acreditación.*

1. La acreditación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio.

2. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme a lo establecido en el presente Reglamento.

Artículo 98. *Certificación del producto evaluado en el proceso de auditoría.*

Las evaluaciones utilizadas como prueba, en el proceso de auditoría del laboratorio, podrán servir de base para la correspondiente certificación de la seguridad de los productos evaluados, conforme a lo indicado en el Capítulo V.

Sección 5.ª Seguimiento de la actividad de evaluación

Artículo 99. *Seguimiento continuo de la actividad de evaluación.*

El Organismo de Certificación, conforme al procedimiento de certificación de productos, establecido en el Capítulo V, realizará un seguimiento continuo de la actividad del laboratorio, a los efectos de la resolución de las solicitudes de certificación de productos.

Todas aquellas observaciones y disconformidades sobre los requisitos de acreditación del laboratorio, detectadas durante el seguimiento de las evaluaciones, serán comunicadas al laboratorio para su subsanación.

En el caso de disconformidad, o de no atender las observaciones realizadas, se estará a lo dispuesto en los artículos 104, 105 y 106.

Artículo 100. *Auditorías de seguimiento.*

1. De forma periódica, se realizarán auditorías de seguimiento a los laboratorios acreditados.

2. Los objetivos de las auditorías de seguimiento serán los siguientes:

a) Comprobar que la entidad ha respetado, durante el periodo transcurrido desde la última auditoría, los criterios establecidos para la concesión de la acreditación.

b) Verificar el cierre de las desviaciones detectadas en auditorías previas.

c) Examinar cualquier cambio en la organización, procedimientos y recursos de la entidad, para la realización de las actividades incluidas en el alcance de su acreditación.

d) Comprobar que se han respetado las obligaciones resultantes de la acreditación.

e) Comprobar la actividad de la entidad para el alcance acreditado.

3. La frecuencia de las auditorías se establecerá en función de los resultados de visitas previas.

4. La primera auditoría de seguimiento se programará en un plazo no superior a doce meses desde la fecha inicial de acreditación. Las siguientes auditorías de seguimiento se realizarán antes de transcurridos dieciocho meses desde la realización de la última visita.

5. Las auditorías de seguimiento se realizarán con el mismo grado de detalle y rigor que la auditoría inicial de acreditación.

6. En la instrucción y resolución de la auditoría de seguimiento se seguirá lo dispuesto en los artículos 93 y 94 y, en todo caso, se atendrá al procedimiento general administrativo.

Artículo 101. *Ampliación del alcance de una acreditación.*

Cuando un laboratorio, ya acreditado, desee ampliar el alcance de su acreditación deberá solicitar formalmente dicha ampliación. Para ello, deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento indicado en el artículo 78 adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

Artículo 102. *Notificación de cambios.*

1. El laboratorio deberá comunicar, al Organismo de Certificación, cualquier cambio que se proponga efectuar sobre las condiciones iniciales en que se concedió la acreditación y, en particular, los que afecten a lo siguiente:

a) Situación jurídica, comercial u organizativa del laboratorio.

b) Organización y gestión, cuando afecten a personal directivo o a puestos clave en la organización del laboratorio o de la empresa.

c) Políticas y procedimientos, cuando proceda.

d) Locales de ubicación del laboratorio.

e) Personal y otros recursos, cuando sean relevantes.

f) Documentos normativos incluidos en el alcance de la acreditación.

2. Ante una comunicación de cambio, el Organismo de Certificación procederá a su revisión y establecerá las actividades necesarias para el mantenimiento de la acreditación del laboratorio. Dichas actividades podrán consistir en acciones de auditoría, por parte del Organismo de Certificación, para comprobar el grado de cumplimiento de los requisitos de acreditación tras los cambios efectuados, así como en la actualización, por parte del laboratorio, de la documentación presentada en el proceso de acreditación.

Artículo 103. *Publicidad de las acreditaciones.*

El Organismo de Certificación podrá hacer pública la relación de laboratorios en proceso de acreditación, así como la de laboratorios acreditados incluyendo, en esta relación, la información del alcance de cada acreditación.

Sección 6.ª Formulación de observaciones, plazos y recursos

Artículo 104. *Formulación de observaciones y retirada de la acreditación.*

El incumplimiento de las obligaciones derivadas de la acreditación, por parte de la entidad titular de la misma, dará lugar a la adopción de medidas, por parte del Organismo de Certificación, contra la entidad incumplidora.

Las medidas irán en función de la gravedad del incumplimiento y podrán consistir en formulación de observaciones, retirada parcial o retirada total de la acreditación.

Artículo 105. *Actuaciones irregulares e incumplimientos.*

Se entenderá por actuaciones irregulares e incumplimientos leves, aquellas actuaciones que, sin adecuarse a lo establecido en el presente Reglamento, no afecten a la validez final de la actividad de evaluación de la entidad ni a la seguridad de terceros.

Las actuaciones irregulares y los incumplimientos leves serán objeto de observación, que podrá notificarse por los equipos de auditoría y seguimiento de las evaluaciones. El

laboratorio deberá subsanar la causa que dio lugar a las observaciones, en el plazo de diez días.

Artículo 106. *Retirada de la acreditación.*

El incumplimiento reiterado de los requisitos de acreditación, o la no subsanación reiterada de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la acreditación a la que se refiera.

La resolución de retirada de acreditación se dictará, de oficio, por el Organismo de Certificación.

La retirada de la acreditación obligará al solicitante al cese inmediato del uso de la condición de laboratorio acreditado, así como a la retirada de esta condición en todos los documentos o información en los que éste la haga manifiesta.

Artículo 107. *Plazos y actos presuntos.*

El plazo para resolver la solicitud de acreditación de laboratorio, y notificar la correspondiente resolución, será de seis meses. Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una acreditación previa.

A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las solicitudes de acreditación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

Artículo 108. *Recursos.*

La actuación del Organismo de Certificación debe siempre atenerse a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, así como en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de acreditación, se podrá interponer:

a) En el plazo de un mes, recurso potestativo de reposición ante el Director de dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

CAPÍTULO V

Certificación de productos y sistemas

Sección 1.ª Certificación

Artículo 109. *Certificación de seguridad de productos y sistemas.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información, siguiendo el procedimiento establecido en este Capítulo y tras considerar, entre otras pruebas de la instrucción del procedimiento, los informes de evaluación emitidos por los laboratorios acreditados conforme a lo establecido en el Capítulo IV, y realizados atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI.

Artículo 110. *Reconocimiento de veracidad de propiedades de seguridad.*

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de su correspondiente declaración de seguridad.

Artículo 111. *Valoración de idoneidad.*

La certificación de la seguridad de un producto o sistema no presupone declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad de un producto o sistema deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en su declaración de seguridad para la correcta interpretación del certificado.

Artículo 112. *Vigencia de la certificación.*

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos, aparición de nuevas vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el propio producto o renuncia expresa del solicitante. Para la vigilancia de la vigencia de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del producto, de su entorno y del uso del certificado.

Sección 2.ª Alcance de la certificación

Artículo 113. *Alcance de la certificación.*

La certificación se limita mediante el correspondiente alcance, que incluye la definición del producto evaluado y las normas y niveles de evaluación.

El Organismo de Certificación, en la determinación del alcance, realizará la definición más precisa posible del mismo, al objeto de evitar confusión alguna entre el producto comercial y el producto evaluado, en el supuesto de que ambos no coincidan exactamente.

Artículo 114. *Alcance con relación al producto o sistema evaluado.*

La certificación deberá hacer referencia, e identificar inequívocamente, al producto evaluado, así como a su declaración de seguridad. Dicha declaración de seguridad también deberá contener la identificación precisa del producto evaluado, así como la especificación de su entorno de uso, incluyendo las amenazas previstas, políticas de seguridad e hipótesis aplicables al caso, además de los objetivos de seguridad del producto o sistema y la relación de requisitos de seguridad exigibles al mismo.

Los detalles de la declaración de seguridad podrán variar conforme a las normas aplicadas en la evaluación, pero toda declaración deberá ser un reflejo cierto, claro y preciso de las propiedades de seguridad del producto o sistema evaluado.

Artículo 115. *Alcance con relación a las normas y niveles de evaluación.*

La certificación incluirá en su alcance los criterios, métodos y normas de evaluación empleados en la evaluación del producto o sistema, así como el nivel que se haya alcanzado, de los definidos en cada norma, y la relación de interpretaciones e instrucciones técnicas aplicadas.

Sección 3.ª Criterios de certificación

Artículo 116. *Informe técnico de evaluación.*

La principal prueba en la instrucción del procedimiento de certificación es el Informe Técnico de Evaluación, emitido por el laboratorio acreditado y realizado cumpliendo con el procedimiento de certificación, establecido en la siguiente Sección.

Artículo 117. *Criterios complementarios.*

1. En el ejercicio de su función evaluadora, el Organismo de Certificación podrá, a su criterio, realizar análisis, pruebas, inspecciones y auditorías al laboratorio, al producto a

evaluar y al solicitante de la certificación, en los aspectos y requisitos de garantía de seguridad que les sean de aplicación según los criterios y métodos de evaluación utilizados.

2. En particular, será atribución indelegable del Centro Criptológico Nacional el análisis, valoración y acreditación de los algoritmos y medios de cifra que utilice el producto a evaluar.

3. Igualmente, el seguimiento de la evaluación permitirá, al Organismo de Certificación, determinar el ajuste de la evaluación a los procedimientos derivados de las normas aplicables y, por tanto, el ajuste del Informe de Evaluación a las mismas.

Sección 4.ª Procedimiento de certificación

Artículo 118. *Proceso de certificación.*

Aquellos interesados que deseen certificar la seguridad de un producto o sistema de Tecnologías de la Información, deberán someterse al proceso establecido en la presente Sección.

Artículo 119. *Solicitud de certificación.*

1. La solicitud de certificación deberá remitirse al Director del Organismo de Certificación incluyendo en la misma, como mínimo, la siguiente información debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.

b) Nombre del responsable del solicitante y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evidencias y pruebas documentales aportadas.

c) Declaración responsable de conocer y aceptar los términos y requisitos aplicables a la certificación solicitada, incluyendo los derechos de acceso, publicación y limitación de la información de las evaluaciones por parte del Organismo de Certificación.

d) Identificación del laboratorio, acreditado por el Organismo de Certificación, que realizará la evaluación técnica de la seguridad del producto o sistema cuya certificación se solicita.

e) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de desarrollo o integración del producto a evaluar.

f) Alcance de la certificación solicitada, indicando el producto a evaluar y su versión, así como las normas y niveles de evaluación aplicables.

g) Justificante del pago de las tasas de certificación en vigor.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Junto a la solicitud de certificación, se remitirá al Organismo de Certificación la declaración de seguridad, o perfil de protección en su caso, del producto a evaluar y, cuando esto sea posible, una unidad, copia o ejemplar de este último.

3. Paralelamente a la solicitud, el solicitante gestionará con el laboratorio acreditado elegido, el plan detallado de la evaluación, así como el contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante.

Artículo 120. *Modelo de solicitud de certificación.*

Las solicitudes de certificación de la seguridad de productos o sistemas de Tecnologías de la Información se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 121. *Subsanación y mejora de la solicitud de certificación.*

1. A la recepción de la solicitud de certificación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

2. En caso de ser necesaria la subsanación o mejora de la solicitud de certificación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Se podrá, igualmente, requerir al solicitante el suministro de unidades, copias o ejemplares adicionales del producto a evaluar, conforme a la naturaleza del mismo y a las necesidades derivadas de los criterios complementarios de certificación indicados en el artículo 117.

4. Será obligación del solicitante mantener actualizados el material y la documentación incluidos en la solicitud de certificación, en poder del Organismo de Certificación, en el caso de que alguno de éstos se modifique a resultas del proceso de evaluación correspondiente.

Artículo 122. *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de certificación, incluyendo en dicha notificación el nombre y los datos de contacto del responsable del procedimiento de certificación.

Artículo 123. *Aprobación del comienzo de la evaluación.*

1. El laboratorio solicitará, al Organismo de Certificación, la autorización para comenzar la actividad de evaluación. La solicitud irá acompañada de:

a) El plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) La copia del contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

2. Para la resolución de la solicitud de autorización, se convocará una reunión con el laboratorio a la que asistirá el personal del laboratorio asignado a la evaluación y el equipo de certificación, designado por el Organismo de Certificación.

En esta reunión se harán las presentaciones oportunas y, por parte del laboratorio, se expondrá el plan y calendario de evaluación, así como los aspectos técnicos más relevantes de la misma.

3. El laboratorio deberá demostrar la adecuación y suficiencia de los medios materiales y humanos asignados a la evaluación, en particular, en lo referente a la formación del personal evaluador en los detalles del alcance de la certificación.

4. El Organismo de Certificación resolverá sobre la autorización del comienzo de la actividad de evaluación, incluyendo la designación del responsable del procedimiento de certificación.

Artículo 124. *Instrucción de la evaluación.*

1. La instrucción de la evaluación comenzará con el desarrollo de los trabajos de evaluación por parte del laboratorio, durante el cual, el Organismo de Certificación realizará el seguimiento de la actividad de evaluación del producto o sistema cuya certificación se ha solicitado.

Para la realización de este seguimiento, el Organismo de Certificación recibirá, del laboratorio, la información de la evaluación indicada en la Sección 3.ª del Capítulo III, a la vista de la cual convocará las reuniones de seguimiento que considere oportunas. En particular, será de especial atención el ajuste de la ejecución de la evaluación al correspondiente plan de evaluación.

2. La instrucción de la evaluación terminará con el Informe Técnico de Evaluación, que remitirá el laboratorio al Organismo de Certificación, en los siguientes casos:

a) Al término del plazo de evaluación.

b) Por solicitud del Organismo de Certificación. Dicha solicitud se podrá cursar cuando se haya superado, sin subsanar, el plazo de tres meses de cualquier observación o

disconformidad, notificada al solicitante de la certificación, o a los tres meses de retraso no justificado del plan de evaluación.

Artículo 125. *Informe de certificación.*

El Organismo de Certificación, en un plazo no superior a treinta días contados desde la fecha de la recepción del Informe Técnico de Evaluación, elaborará un informe con los resultados y conclusiones de la evaluación, así como de la actividad de seguimiento, que será enviado al solicitante de la certificación para su conocimiento.

Artículo 126. *Audiencia previa a la resolución.*

1. Terminada la instrucción de la evaluación, se pondrá de manifiesto al solicitante de la certificación, convocándole a una reunión de audiencia previa a la resolución.
2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades, identificadas durante la instrucción del expediente de certificación, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de certificación.
3. El solicitante de la certificación, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.
4. Si antes del vencimiento del plazo, el solicitante manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

Artículo 127. *Resolución de la solicitud de certificación.*

1. La resolución de la solicitud de certificación se dictará de acuerdo con lo indicado en este artículo, y en los plazos establecidos en el artículo 137, del presente Reglamento.

Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

2. Las resoluciones de desestimación serán motivadas. La resolución de certificación contendrá, adicionalmente, los siguientes extremos:

a) Alcance de la certificación concedida.
b) La fecha de la entrada en vigor de la certificación y referencia a su vigencia.

Artículo 128. *Vigencia de la certificación.*

La certificación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del solicitante.

Para el mantenimiento de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias revisiones de su vigencia y actividades de vigilancia del uso del certificado, conforme a lo establecido en el artículo 129 siguiente.

Artículo 129. *Revisiones de vigencia.*

Cada dos años se realizará una revisión de la vigencia de cada certificado emitido. El objeto de dicha revisión es la comprobación de que el entorno de uso del producto certificado no ha sufrido variaciones, tales como cambios tecnológicos, aparición de vulnerabilidades o cualquier otro aspecto que pueda invalidar las hipótesis, análisis de riesgos y políticas de seguridad reflejadas en dicho entorno de uso.

La revisión de la vigencia de los certificados podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

Sección 5.ª Seguimiento del uso de los certificados

Artículo 130. *Seguimiento continuo del uso del certificado.*

El Organismo de Certificación realizará un seguimiento continuo del uso de los certificados emitidos, mediante el análisis y registro de toda información comercial o técnica de la que tenga conocimiento y que haga referencia a la certificación emitida.

El incumplimiento de las condiciones de uso del certificado, reguladas en el Capítulo VII, podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

Artículo 131. *Ampliación del alcance de la certificación.*

Cuando se desee ampliar el alcance de la certificación de un producto o sistema, el interesado solicitará formalmente dicha ampliación. Para ello deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento de certificación, indicado en el Capítulo V, adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

Artículo 132. *Notificación de cambios.*

El solicitante de la certificación deberá comunicar al Organismo de Certificación los cambios que identifique, relativos al entorno de seguridad del producto certificado, así como cualquier otro cambio fundamental que se produjese en las condiciones iniciales en que se concedió la certificación.

Artículo 133. *Publicidad de las certificaciones.*

El Organismo de Certificación podrá hacer pública la relación de productos en proceso de evaluación y la de productos certificados, incluyendo en esta relación la declaración de seguridad de los mismos, así como información derivada del informe de certificación establecido en el artículo 125.

Sección 6.ª Formulación de observaciones, plazos y recursos

Artículo 134. *Observaciones y retirada de la certificación.*

El incumplimiento, por un solicitante, de las obligaciones derivadas de la certificación dará lugar, en función de la gravedad de la infracción, a la formulación de observaciones o a la retirada de la certificación.

Artículo 135. *Actuaciones irregulares e incumplimientos.*

Las actuaciones irregulares y los incumplimientos leves, entendiéndose por tales los que no desvirtúen las restricciones y obligaciones derivadas del uso de la condición de producto certificado, serán objeto de observación, que se notificará, de oficio, al solicitante de la certificación.

El solicitante de la certificación deberá subsanar la causa de tales observaciones en un plazo de diez días.

Artículo 136. *Retirada de la certificación.*

1. La disconformidad sostenida, en relación con las restricciones y obligaciones del uso de la condición de producto certificado o con los requisitos para la certificación, así como la falta de subsanación de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la certificación a la que se refiera.

2. La resolución de retirada de certificación se dictará, de oficio, por el Organismo de Certificación.

3. La retirada de la certificación obligará al solicitante al cese inmediato del uso de la condición de producto certificado, en todos los documentos o información en los que la haga manifiesta, y a la retirada del mercado de los productos así etiquetados.

Artículo 137. *Plazos y actos presuntos.*

1. El plazo para resolver la solicitud de certificación de productos, y notificar la correspondiente resolución, será de dos meses, contados a partir de la fecha de recepción del Informe Técnico de Evaluación del laboratorio.

Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una certificación previa.

2. El plazo para resolver la solicitud de comienzo de evaluación, y notificar la correspondiente resolución, será de un mes.

3. A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, las solicitudes de certificación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

Artículo 138. *Recursos.*

La actuación del Organismo de Certificación se atendrá a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, y en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de certificación, los interesados podrán interponer:

a) En el plazo de un mes, recurso potestativo de reposición, ante el Director del dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

CAPÍTULO VI

Criterios y metodologías de evaluación

Artículo 139. *Estado del arte.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información conforme al estado del arte más avanzado en materia de evaluación de la seguridad. Dicho estado del arte se ha de combinar con el debido reconocimiento de los certificados emitidos.

A tal fin, el Organismo de Certificación exigirá a los laboratorios acreditados la realización de su actividad conforme a criterios, métodos y normas bien establecidos y reconocidos. Tales normas se podrán ver complementadas por interpretaciones o instrucciones técnicas emitidas por el Organismo de Certificación.

Artículo 140. *Normas de evaluación.*

1. El Organismo de Certificación, a los efectos de su utilización y cumplimiento por parte de los laboratorios, elevará a carácter de norma cualquier documento de orden técnico que sea de su interés, mediante la publicación del mismo en su dirección electrónica (http://www.oc.ccn.cni.es) y su comunicación a los laboratorios acreditados.

2. La publicación de una nueva norma, o la actualización de una existente, y la determinación de su entrada en vigor, se realizarán previa presentación a los laboratorios acreditados de las nuevas normas y de sus diferencias técnicas con respecto a las normas vigentes, a los efectos que pudieran derivarse sobre las acreditaciones en vigor.

3. Las normas relacionadas en el artículo 141 siguiente, se entienden de aplicación en su última versión disponible al comienzo de cada solicitud de certificación. No obstante lo anterior, se podrá consultar la relación de normas, criterios, metodologías y requisitos, así como su aplicabilidad, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 141. *Criterios de evaluación.*

Los criterios de evaluación serán los recogidos en las siguientes normas:

a) «Common Criteria for Information Technology Security Evaluation» (abreviado, CC).
b) ISO/IEC 15408, «Evaluation Criteria for IT Security».
c) «Information Technology Security Evaluation Criteria» (abreviado, ITSEC). Office for Official Publications of the European Communities.

Artículo 142. *Metodologías de evaluación.*

Las metodologías de evaluación serán las recogidas en las siguientes normas:

a) «Common Methodology for Information Technology Security Evaluation» (abreviado, CEM).
b) ISO/IEC 18045, «Methodology for IT Security Evaluation».
c) «Information Technology Security Evaluation Manual» (abreviado, ITSEM). Office for Official Publications of the European Communities.

Artículo 143. *Requisitos de seguridad específicos.*

Los requisitos de seguridad específicos serán los recogidos en la norma ISO/IEC 19790, «Requisitos de Seguridad para Módulos Criptográficos».

Artículo 144. *Interpretaciones e instrucciones técnicas.*

Se podrá consultar la relación de interpretaciones e instrucciones técnicas en vigor, de aplicación en este Esquema, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es), agrupadas por la norma principal a la que afectan y sus versiones aplicables.

CAPÍTULO VII

Uso de la condición de laboratorio acreditado y de producto certificado

Artículo 145. *Referencia a la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado, o el uso del distintivo correspondiente, en los informes emitidos como resultado de las actividades de evaluación amparadas por la acreditación, es el medio por el cual los laboratorios acreditados declaran públicamente el cumplimiento de todos los requisitos de acreditación en la realización de dichas evaluaciones.

Cualquier uso que no esté expresamente permitido en este Reglamento deberá ser consultado al Organismo de Certificación.

Artículo 146. *Informes derivados de la evaluación.*

1. La referencia a la condición de laboratorio acreditado debe ser utilizada en todos los informes emitidos como resultado de las actividades de evaluación, amparadas por la acreditación, como garantía del cumplimiento de los requisitos de dicha acreditación.

2. Cualquier informe o certificado que no incluya la referencia a la condición de laboratorio acreditado, no garantiza el cumplimiento de los requisitos de acreditación y, por tanto, no será aceptado por el Organismo de Certificación, como parte de una evaluación acreditada, ni podrá beneficiarse del reconocimiento de los certificados emitidos por el Organismo de Certificación.

3. En el caso de informes que incluyan, tanto datos amparados por la acreditación, como datos no amparados por la misma, se seguirán las siguientes reglas:

a) Se señalarán los datos no amparados por la acreditación mediante la utilización de un asterisco o similar. Asimismo, se deberá incluir en un lugar visible la siguiente leyenda: «Los ensayos/inspecciones marcados no están incluidos en el alcance de acreditación».

b) Cuando un informe de evaluación contenga interpretaciones, opiniones o cualquier otra información relativa a investigación, que no sea parte de la metodología de ensayo seguida en esa evaluación, se deberá incluir la siguiente advertencia: «Las opiniones, interpretaciones, etc., que se indican a continuación, están fuera del alcance de la acreditación del Organismo de Certificación».

Artículo 147. *Otros documentos de laboratorio acreditado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con la actividad de evaluación acreditada, o en material de papelería (papel de cartas, impresos tales como facturas o pedidos, sobres, etc.), los laboratorios podrán usar la referencia a la condición de acreditado con las restricciones que se mencionan en el artículo 148.

Artículo 148. *Restricciones al uso de la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado no se debe utilizar en los siguientes supuestos:

a) En informes o certificados que no contengan ningún dato obtenido de actividades acreditadas.

b) En documentos en los que no se identifique la organización a la que ha sido concedida la acreditación.

c) De forma que pueda sugerir que el Organismo de Certificación aprueba, acepta o, de alguna manera, se responsabiliza de los resultados contenidos en un informe o certificado (por ejemplo, mediante el uso de sellos con la referencia al Organismo de Certificación).

d) Cuando el laboratorio haya perdido su condición de acreditado, ya sea de forma voluntaria o por retirada de la acreditación.

e) En las tarjetas de visita del personal de los laboratorios acreditados.

f) En cualquier situación que pueda dar lugar a una interpretación incorrecta de la condición del laboratorio acreditado, o que pueda inducir a considerar actividades no acreditadas como cubiertas por la acreditación. Concretamente:

1.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, páginas Web, etc.), que hagan referencia a actividades no acreditadas, se deberá incluir una mención, con el mismo tamaño de letra que el usado en el cuerpo del documento en cuestión, en la que se aclare este hecho (por ejemplo: «Las actividades recogidas en el presente escrito no están incluidas en el alcance de la acreditación del Organismo de Certificación»).

2.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, etc.), que incluyan tanto actividades acreditadas como no acreditadas, su uso deberá ser tal, que permita al lector distinguir aquellas actividades que están acreditadas de las que no lo están.

3.º Cuando un laboratorio esté compuesto por varios emplazamientos distintos, y no todos ellos hayan sido acreditados, solamente aquellos que sí lo hayan sido podrán hacer uso de la referencia a la condición de acreditado. Cuando se emitan documentos comunes a todo el laboratorio se deberá incluir una cláusula que indique esta condición (por ejemplo: «Se encuentra disponible la lista de emplazamientos acreditados y sus alcances»).

4.º Cuando una organización acreditada pertenezca a otra mayor, no deberá existir confusión sobre cual de ellas está acreditada.

g) En cualquier otro supuesto que resulte abusivo, a juicio del Organismo de Certificación.

Artículo 149. *Uso de la condición de producto certificado.*

El uso del distintivo especificado en el artículo 155, o la referencia a la condición de producto certificado, es el medio por el cual los solicitantes de la certificación declaran, públicamente, el cumplimiento de todos los requisitos exigibles para dicha certificación, la conformidad con determinados perfiles de protección, en su caso, y el cumplimiento de las disposiciones legales aplicables.

Cualquier uso del certificado que no esté expresamente permitido en este Reglamento, deberá ser consultado al Organismo de Certificación.

Artículo 150. *Producto y documentación.*

La referencia a la condición de producto certificado debe ser utilizada en toda la documentación de administración y uso de dicho producto, y que se haya remitido como evidencia de la evaluación.

La referencia a la condición de producto certificado se incluirá también en el propio producto, siguiendo las reglas de marcado indicadas en el artículo 155.

Artículo 151. *Otros documentos de producto certificado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con el producto certificado, así como en los contratos públicos y privados, licitaciones y documentación preparatoria, el titular de la certificación podrá usar la referencia a la condición de producto certificado con las restricciones que se mencionan en el artículo 152.

Artículo 152. *Restricciones al uso de la condición de producto certificado.*

La referencia a la condición de producto certificado no debe utilizarse en los siguientes supuestos:

a) Sin una referencia completa e inequívoca del alcance del certificado. Como mínimo se citará:

1.º Nombre y versión del producto evaluado.

2.º La norma utilizada para la evaluación y el nivel alcanzado en la misma (por ejemplo: ISO/IEC 15408 EAL2).

3.º Referencia a la declaración de seguridad del producto certificado, indicando el procedimiento para obtener una copia de la misma.

b) De forma que pueda sugerir que el certificado se aplica a todo un sistema o producto, cuando el producto evaluado es sólo una parte del mismo.

c) De forma que se sugieran propiedades de seguridad del producto certificado no reflejadas en su declaración de seguridad.

d) Cuando el certificado haya sido anulado por cualquier motivo.

e) En cualquier otro uso que resulte abusivo a juicio del Organismo de Certificación.

Artículo 153. *Otras obligaciones de la condición de producto certificado.*

La referencia a la condición de producto certificado obligará al solicitante de la certificación a:

a) Mantener registro de todas las reclamaciones presentadas al solicitante, relativas a la seguridad del producto certificado, y a tener esta información disponible para el Organismo de Certificación.

b) Tomar las acciones correctoras apropiadas con respecto a tales reclamaciones y a cualquier deficiencia encontrada en los productos, que afecten la conformidad con los requisitos para la certificación.

c) Documentar las acciones tomadas.

Artículo 154. *Distintivo de laboratorio acreditado.*

La condición de laboratorio acreditado puede complementarse mediante el uso del distintivo descrito a continuación (figura 2):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «LABORATORIO ACREDITADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm.

Figura 2. Distintivo de laboratorio acreditado

Artículo 155. *Distintivo de producto certificado.*

Los productos certificados deberán llevar un distintivo conforme a lo siguiente (figura 3):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «PRODUCTO CERTIFICADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm, excepto cuando esto no sea posible a causa del tipo de producto.

Figura 2. Distintivo de producto certificado con indicación del alcance

h) El distintivo deberá colocarse en el producto o en su placa informativa. Además, deberá colocarse en el embalaje, si existe, y en la documentación que le acompañe. En productos software, se mostrará el distintivo donde se haga referencia a la versión particular del producto.

i) El distintivo deberá colocarse de forma visible, legible e indeleble.

j) Se incluirá un elemento destinado a informar al usuario sobre el alcance de la certificación (norma y nivel aplicados en la evaluación).

§ 6

Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social

Ministerio de Empleo y Seguridad Social
«BOE» núm. 117, de 14 de mayo de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-5111

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el derecho de los ciudadanos a relacionarse con las administraciones públicas a través de medios electrónicos, comportando una obligación para éstas de promover las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

Dicha ley determina que el Esquema Nacional de Seguridad tendrá por objeto establecer la política de seguridad en la utilización de medios electrónicos y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, entiende por seguridad un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Esta disposición reglamentaria obliga a todos los órganos superiores de las administraciones públicas a disponer formalmente de su política de seguridad, comprometiendo a todos los miembros de la organización.

En base a tales previsiones normativas, se dictaron la Orden TIN/3016/2011, de 28 de octubre, por la que se creó el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

La Secretaría de Estado de la Seguridad Social, órgano superior del Ministerio de Empleo y Seguridad Social, ha establecido mediante Resolución de 2 de septiembre de 2013, de la Secretaría de Estado de la Seguridad Social, por la que se aprueba la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social, su política de seguridad identificando unos claros responsables de velar por su cumplimiento. La proliferación de los sistemas de información de los organismos adscritos y de los órganos dependientes de la Secretaría de Estado y la interconexión entre ellos, hace aconsejable la creación de un Comité de Seguridad de los Sistemas de Información en el ámbito de la Seguridad Social, como órgano colegiado con funciones de coordinación de aquéllos y de propuesta y aprobación de las medidas conducentes al cumplimiento de la política de seguridad a que obliga el Esquema Nacional de Seguridad.

En la tramitación de esta orden se ha obtenido el informe favorable del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Creación y adscripción del Comité de Seguridad de los Sistemas de Información de la Seguridad Social.*

Se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social (en adelante CSISS) como órgano colegiado adscrito a la Secretaría de Estado de la Seguridad Social.

Artículo 2. *Funciones.*

El CSISS coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito de la Secretaría de Estado y se comunicará con el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social (en adelante CSTIC), ejerciendo las siguientes funciones:

1. Definir y elevar para su aprobación al CSTIC los planes estratégicos, líneas de actuación y objetivos en materia de seguridad en la Secretaría de Estado de la Seguridad Social, siempre alineados con la misión y objetivos de la organización.
2. Garantizar la divulgación de la política de seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social.
3. La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente a la Administración de la Seguridad Social.
4. Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.
5. Revisar el estado global de la seguridad en cada uno de los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado, y elevar los informes pertinentes al CSTIC cuando sea necesario.
6. Trasladar las directrices que sean establecidas desde el CSTIC a cada uno de los órganos directivos y garantizar su cumplimiento.
7. Actualizar y asignar las funciones y obligaciones de cada uno de los responsables definidos en la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.
8. Promover las líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal de la Secretaría de Estado de la Seguridad Social.
9. Ser informado, deliberar e intercambiar información con los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado y que sean responsables de ficheros con datos personales para tratar y asesorar sobre las medidas de seguridad técnica aplicables en los sistemas y servicios que les afecten y que utilicen tecnologías de la información y comunicaciones.

Artículo 3. *Composición.*

El CSISS estará compuesto por los siguientes miembros:

1. Presidente: El Secretario de Estado de la Seguridad Social o persona que le sustituya.
2. Vocales: un representante designado por los titulares de cada uno de los siguientes órganos:

a) Gabinete de la Secretaría de Estado de la Seguridad Social.
b) Dirección General de Ordenación de la Seguridad Social.
c) Intervención General de la Seguridad Social.
d) Instituto Nacional de la Seguridad Social.
e) Tesorería General de la Seguridad Social.
f) Instituto Social de la Marina.
g) Servicio Jurídico de la Administración de la Seguridad Social.

h) Gerencia de Informática de la Seguridad Social.

Estos vocales deberán tener rango de subdirector general o asimilado, entendiéndose también por tales quienes ejerzan competencias en materia de seguridad de los sistemas de información en los órganos anteriores.

3. Secretaría: Con voz y sin voto, será designada por la Gerencia de Informática de la Seguridad Social.

Artículo 4. *Funcionamiento.*

El CSISS se reunirá con carácter ordinario como mínimo tres veces al año o, con carácter extraordinario, cuando el Presidente lo considere necesario.

En caso de ser necesario, y por invitación del Presidente del CSISS, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estimen convenientes.

En todo caso, se aplicará con carácter supletorio lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición adicional única. *No incremento del gasto público.*

La creación y el funcionamiento del Comité de Seguridad de los Sistemas de Información de la Seguridad Social serán atendidos con los medios personales, técnicos y presupuestarios asignados a la Secretaría de Estado de la Seguridad Social.

Disposición final única. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 7

Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración

Ministerio de Trabajo e Inmigración
«BOE» núm. 271, de 10 de noviembre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-17656

Vivimos en una época que ha visto la generalización de la sociedad de la información a todos los niveles y la Administración Pública no se ha visto excluida de esta realidad, más bien al contrario, ha tratado no solo de utilizar los medios tecnológicos necesarios para formar parte de la sociedad de la información, sino también de impulsar el uso de dichos medios en la sociedad en general y en las relaciones de los ciudadanos con la Administración en particular.

Ya en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se menciona el impulso al uso de medios electrónicos para el desarrollo de su actividad y el ejercicio de sus competencias y también determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones electrónicas.

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y posteriormente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo ponen de relieve que el uso de medios electrónicos conlleva unas necesidades de seguridad especifica de estos medios traducidas en una serie de medidas concretas aplicables a cualquier sistema de información que trate datos de carácter personal.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos consagra el derecho de los ciudadanos a comunicarse electrónicamente con la Administración Pública, dando respuesta también a los compromisos comunitarios y a las iniciativas europeas puestas en marcha a partir de Consejo Europeo de Lisboa. Esta Ley manifiesta la necesidad de una adecuada protección de la información y de los servicios que permita usar los medios electrónicos con confianza y a esta necesidad responde la publicación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El Esquema Nacional de Seguridad tiene como finalidad crear las condiciones de confianza necesarias en el uso de los medios electrónicos, mediante medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Actualmente los sistemas de información de las Administraciones Públicas están fuertemente imbricados entre sí,

siendo la seguridad una función transversal a todos ellos, por lo que la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Por ello, entre las obligaciones que impone el mencionado Esquema Nacional se encuentran la de que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que será aprobada por el titular del órgano superior correspondiente, impulsar y verificar la realización de auditorías periódicas de los sistemas de información e informar del estado de la seguridad a los órganos competentes. En el citado Real Decreto 3/2010 de 8 de enero, en el anexo II, apartado 3.1.d), Política de seguridad, se establece la existencia de un comité para la gestión y coordinación de la seguridad.

Esta orden ministerial desarrolla el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración cuyo objetivo es establecer, gestionar, coordinar y aprobar las actuaciones en materia de seguridad de las tecnologías de la información y las comunicaciones, incluyendo dentro del ámbito de actuación del mismo a todos los sistemas de información del Ministerio de Trabajo e Inmigración, de manera que se gestione de forma conjunta la seguridad de dichos sistemas. El motivo es el carácter horizontal de la seguridad y la fuerte interconexión entre todos los sistemas de información que permiten a la Administración Pública prestar su servicio a los ciudadanos.

En el funcionamiento del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración deberá promoverse la utilización de medios electrónicos, de conformidad con lo establecido en la disposición adicional primera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

En su virtud, y con la aprobación previa del Vicepresidente del Gobierno de Política Territorial y Ministro de Política Territorial y Administración Pública, dispongo:

Artículo 1. *Creación y adscripción del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.*

Se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante TIC) del Ministerio de Trabajo e Inmigración como órgano colegiado de carácter transversal, adscrito a la Subsecretaría de Trabajo e Inmigración.

Artículo 2. *Estructura del Comité de Seguridad TIC del Ministerio de Trabajo e Inmigración.*

El Comité de Seguridad TIC del Ministerio de Trabajo e Inmigración se estructura a través de: Comité de Dirección de Seguridad TIC (en adelante CDSTIC) y Comité Permanente de Seguridad TIC (en adelante CPSTIC).

Artículo 3. *Funciones del Comité de Dirección de Seguridad TIC.*

Al CDSTIC le corresponde, en el ámbito del Ministerio de Trabajo e Inmigración, determinar y coordinar el mandato contenido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y, por tanto la política de seguridad que se ha de implementar en el Departamento para la utilización de los medios electrónicos de forma que se garantice una adecuada protección de la información. En concreto le corresponde:

1. La dirección y seguimiento de la aplicación de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de las TIC.
2. La aprobación y seguimiento de las Políticas, los planes estratégicos, planes directores y líneas de actuación del Departamento en materia de seguridad TIC que proponga el Comité Permanente.
3. La aprobación y seguimiento de las normativas en materia de seguridad, que afecten transversalmente a toda la organización. Así como, impulsar nuevas líneas en materia de seguridad de las Tecnologías de la Información y las Comunicaciones
4. La aprobación y seguimiento de las políticas de auditoría de las Unidades del Departamento, a propuesta del Comité Permanente.

5. La aprobación de las declaraciones de aplicabilidad y conformidad con el Esquema Nacional de Seguridad de cada una de las Unidades del Ministerio de Trabajo e Inmigración, a propuesta del Comité Permanente.

6. Designar la representación e informar sobre el estado de la seguridad TIC del Ministerio de Trabajo e Inmigración, en el Comité de Seguridad de la Información de las Administraciones Públicas definido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

7. El control de las actuaciones del CPSTIC y atribuir o delegar en el mismo las competencias que estime oportuno.

8. El impulso de nuevas líneas de trabajo en materia de seguridad de las TIC.

Artículo 4. *Composición del Comité de Dirección de Seguridad TIC.*

1. Presidencia: Subsecretario de Trabajo e Inmigración.

2. Vocales, serán representantes que ocupen puestos de nivel 30 o superior:

a) Dos representantes designados por el titular de la Subsecretaría de Trabajo e Inmigración.

b) Dos representantes designados por el titular de la Secretaría de Estado de la Seguridad Social.

c) Dos representantes designados por el titular de la Secretaría de Estado de Empleo.

d) Dos representantes designados por el titular de la Secretaría de Estado de Inmigración y Emigración.

e) Un representante designado por el titular de la Dirección General de la Inspección de Trabajo y Seguridad Social.

f) El titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, que además actuará como Secretario del CDSTIC.

Artículo 5. *Funcionamiento del Comité de Dirección de Seguridad TIC.*

El CDSTIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando el Presidente lo decida o sí:

1. Surgieran incidencias de seguridad graves que afecten al Ministerio de Trabajo e Inmigración.

2. Fuera necesario establecer nuevas directrices de seguridad que afecten a todo el Departamento.

3. Existiera una solicitud motivada del CPSTIC.

La secretaría del CDSTIC levantará acta de las reuniones, siendo enviadas a la Presidencia de dicho comité para su aprobación, en su caso, en el pleno siguiente. Esta Secretaría realizará todos los trabajos previos necesarios para las reuniones del CDSTIC, apoyándose cuando lo requiera en las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e inmigración.

Caso de ser necesario, y por invitación del Presidente del Comité de Dirección, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estime conveniente.

Artículo 6. *Funciones del Comité Permanente de Seguridad TIC.*

Al CPSTIC le corresponde en materia de Seguridad de las TIC, en el ámbito del Ministerio de Trabajo e Inmigración, la ejecución de cuantas tareas le sean encomendadas por el CDSTIC, y en particular:

1. Proponer para su aprobación y seguimiento en el CDSTIC:

a) Los planes estratégicos, planes directores y líneas de actuación en materia de seguridad TIC de las Unidades del Departamento.

b) Las políticas, normas y procedimientos de seguridad de cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e Inmigración.

c) Las políticas de auditoría de las Unidades del Ministerio de Trabajo e Inmigración.

d) Las declaraciones de aplicabilidad y conformidad con el Esquema Nacional de Seguridad de cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e Inmigración.

e) Los indicadores y resultados significativos que en materia de seguridad se determinen, para lo que se podrá recabar la información necesaria de cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e inmigración.

2. Asesorar al CDSTIC en todo lo que solicite y reportar al CDSTIC todas las cuestiones de las que, por su relevancia, deba tener conocimiento.

3. Promover, dirigir y coordinar los proyectos de seguridad que afecten a todo el Departamento.

4. Realizar la aprobación y seguimiento de los sistemas de gestión de la seguridad de cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e Inmigración.

5. Crear y determinar la composición, objetivos y funcionamiento de los grupos de trabajo así como el ámbito de actuación y el periodo de vigencia de los mismos, dando cuenta de ello al CDSTIC. Se habilita al CPSTIC para la creación de cuantos grupos de trabajo considere necesarios.

6. Promover la formación y concienciación en materia de seguridad de las TIC en cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e Inmigración.

7. Informar al CDSTIC sobre el estado de la seguridad de las TIC de cada una de las Unidades, organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social del Ministerio de Trabajo e Inmigración.

Artículo 7. *Composición del Comité Permanente de Seguridad TIC.*

1. Presidencia: El titular de la Subdirección General de Tecnologías de la Información y Comunicaciones

2. Vocales: Será un representante designado por los titulares de cada uno de los siguientes órganos:

a) Subsecretaría de Trabajo e Inmigración
b) Secretaría de Estado de la Seguridad Social
c) Secretaría de Estado de Empleo
d) Secretaría de Estado de Inmigración y Emigración
e) Secretaría General Técnica
f) Gerencia de Informática de la Seguridad Social
g) Subdirección General de Tecnologías de la Información y Comunicaciones del Servicio Público de Empleo Estatal
h) Dirección General de la Inspección de Trabajo y Seguridad Social
i) Fondo de Garantía Salarial
j) Instituto Nacional de Seguridad e Higiene en el Trabajo
k) Subdirección General de Tecnologías de la Información y Comunicaciones

3. Secretaría: Con voz y sin voto, será designada por el titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, entre los funcionarios de dicha Subdirección.

Artículo 8. *Funcionamiento del Comité Permanente de Seguridad de las TIC.*

El CPSTIC se reunirá con carácter ordinario como mínimo dos veces al año o con carácter extraordinario cuando el Presidente lo considere necesario.

La secretaría del CPSTIC levantará acta de las reuniones, siendo enviadas a la Presidencia de dicho Comité para su aprobación, en su caso, en el pleno siguiente. La Presidencia del CPSTIC elevará las actas al CDSTIC.

La Presidencia del CPSTIC, con el apoyo de la Secretaría de este Comité, realizará todos los trabajos previos necesarios para las reuniones del CPSTIC, apoyándose cuando lo requiera en las Unidades, organismos autónomos, entidades gestoras y servicios comunes

de la Seguridad Social del Ministerio de Trabajo e inmigración, de las que podrá recabar cualquier información que precise y con el nivel de detalle que considere necesario.

Caso de ser necesario, y por invitación del Presidente del CPSTIC, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estime conveniente.

Artículo 9. *Funciones, composición y funcionamiento de los grupos de trabajo.*

Las funciones, composición y funcionamiento de cada grupo de trabajo estarán determinadas por el CPSTIC en su acuerdo de creación.

Sus funciones se limitaran al mandato recibido del Comité Permanente.

Disposición adicional primera. *Funcionamiento por medios electrónicos.*

El Comité de Dirección de Seguridad TIC y el Comité Permanente de Seguridad TIC podrán celebrar sus reuniones por medios electrónicos, de conformidad con lo establecido en la disposición adicional primera de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Corresponderá al Presidente de cada uno de los citados órganos colegiados acordar la utilización de dicho procedimiento.

El sistema utilizado deberá asegurar una comunicación confidencial multidireccional en tiempo real y garantizar la identificación inequívoca del respectivo miembro y la autenticidad de su voto en el mismo acto. En particular garantizará el cumplimiento de las siguientes especialidades:

a) La realización efectiva de la convocatoria, el acceso a la información y la comunicación del orden del día, en donde se especificarán los tiempos en los que se organizarán los debates, la formulación y conocimiento de las propuestas y la adopción de acuerdos.

b) El régimen de constitución y adopción de acuerdos garantizará la participación de los miembros del Comité respectivo, de acuerdo con sus normas de funcionamiento.

c) Los registros de las sesiones estarán a disposición de los asistentes, dejarán constancia de las comunicaciones producidas, así como del contenido de los acuerdos adoptados.

Disposición adicional segunda. *No incremento del gasto público.*

La aplicación de esta Orden no conllevará incremento de gasto público, atendiéndose el funcionamiento de los Comités y grupos de trabajo con los recursos humanos y materiales de que dispone el Ministerio de Trabajo e Inmigración.

Disposición final única. *Entrada en vigor.*

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 8

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 8 de noviembre de 2011
Referencia: BOE-A-2010-1331

I

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado. La interoperabilidad se recoge dentro del principio de cooperación en el artículo 4 y tiene un protagonismo singular en el título cuarto dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En dicho título el aseguramiento de la interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas figura en el artículo 40 entre las funciones del órgano de cooperación en esta materia, el Comité Sectorial de Administración Electrónica. A continuación, el artículo 41 se refiere a la aplicación por parte de las Administraciones públicas de las medidas informáticas, tecnológicas y organizativas, y de

seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica. Y, seguidamente, el artículo 42.1 crea el Esquema Nacional de Interoperabilidad que comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

II

El Esquema Nacional de Interoperabilidad tiene presentes las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos, así como en su caso y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre acceso electrónico de los ciudadanos a los servicios públicos, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la administración electrónica. Se han tenido en cuenta otros instrumentos, tales como el Esquema Nacional de Seguridad, desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio, o antecedentes como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades.

En términos de las recomendaciones de la Unión Europea se atiende al Marco Europeo de Interoperabilidad, elaborado por el programa comunitario IDABC, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

III

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

En consecuencia, el Esquema Nacional de Interoperabilidad atiende a todos aquellos aspectos que conforman de manera global la interoperabilidad. En primer lugar, se atiende a las dimensiones organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio; en segundo lugar, se tratan los estándares, que la Ley 11/2007, de 22 de junio, pone al servicio de la interoperabilidad así como de la independencia en la elección de las alternativas tecnológicas y del derecho de los ciudadanos a elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas; en tercer lugar, se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral; en cuarto lugar, se trata la reutilización, aplicada a las aplicaciones

de las Administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz «compartir» se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con «reutilizar», ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar; en quinto lugar, se trata la interoperabilidad de la firma electrónica y de los certificados; por último, se atiende a la conservación, según lo establecido en la citada Ley 11/2007,de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La norma se estructura en doce capítulos, cuatro disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria, tres disposiciones finales y un anexo conteniendo el glosario de términos.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42, apartado 3, y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 2. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

Artículo 3. *Ámbito de aplicación.*

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Interoperabilidad.*

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes principios específicos de la interoperabilidad:

a) La interoperabilidad como cualidad integral.
b) Carácter multidimensional de la interoperabilidad.
c) Enfoque de soluciones multilaterales.

Artículo 5. *La interoperabilidad como cualidad integral.*

La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

Artículo 6. *Carácter multidimensional de la interoperabilidad.*

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Artículo 7. *Enfoque de soluciones multilaterales.*

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

CAPÍTULO III

Interoperabilidad organizativa

Artículo 8. *Servicios de las Administraciones públicas disponibles por medios electrónicos.*

1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999

de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se potenciará el establecimiento de convenios entre las Administraciones públicas emisoras y receptoras y, en particular, con los nodos de interoperabilidad previstos en el apartado 3 de este artículo, con el objetivo de simplificar la complejidad organizativa sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el Comité Sectorial de Administración electrónica se identificarán, catalogarán y priorizarán los servicios de interoperabilidad que deberán prestar las diferentes Administraciones públicas.

2. Las Administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la Red de comunicaciones de las Administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

3. Las Administraciones públicas podrán utilizar nodos de interoperabilidad, entendidos como entidades a las cuales se les encomienda la gestión de apartados globales o parciales de la interoperabilidad organizativa, semántica o técnica.

Artículo 9. *Inventarios de información administrativa.*

1. Las Administraciones públicas mantendrán actualizado un Inventario de Información Administrativa, que incluirá los procedimientos administrativos y servicios que prestan de forma clasificada y estructurados en familias, con indicación del nivel de informatización de los mismos. Asimismo mantendrán una relación actualizada de sus órganos administrativos y oficinas de registro y atención al ciudadano, y sus relaciones entre ellos. Dichos órganos y oficinas se codificarán de forma unívoca y esta codificación se difundirá entre las Administraciones públicas.

2. Cada Administración pública regulará la forma de creación y mantenimiento de este Inventario, que se enlazará e interoperará con el Inventario de la Administración General del Estado en las condiciones que se determinen por ambas partes y en el marco de lo previsto en el presente real decreto; en su caso, las Administraciones públicas podrán hacer uso del citado Inventario centralizado para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

CAPÍTULO IV

Interoperabilidad semántica

Artículo 10. *Activos semánticos.*

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de

mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

CAPÍTULO V

Interoperabilidad técnica

Artículo 11. *Estándares aplicables.*

1. Las Administraciones públicas usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos, al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

a) Los documentos y servicios de administración electrónica que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, disponibles mediante estándares abiertos.

b) Los documentos, servicios electrónicos y aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

2. En las relaciones con los ciudadanos y con otras Administraciones públicas, el uso en exclusiva de un estándar no abierto sin que se ofrezca una alternativa basada en un estándar abierto se limitará a aquellas circunstancias en las que no se disponga de un estándar abierto que satisfaga la funcionalidad satisfecha por el estándar no abierto en cuestión y sólo mientras dicha disponibilidad no se produzca. Las Administraciones públicas promoverán las actividades de normalización con el fin de facilitar la disponibilidad de los estándares abiertos relevantes para sus necesidades.

3. Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:

a) Las definiciones de norma y especificación técnica establecidas en la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. En cualquier caso los ciudadanos podrán elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas, o dirigirse a las mismas, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. Para facilitar la interoperabilidad con las Administraciones públicas el catálogo de estándares contendrá una relación de estándares abiertos y en su caso complementarios aplicables.

CAPÍTULO VI

Infraestructuras y servicios comunes

Artículo 12. *Uso de infraestructuras y servicios comunes y herramientas genéricas.*

Las Administraciones públicas enlazarán aquellas infraestructuras y servicios que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral en el intercambio de información y de servicios entre todas las Administraciones públicas.

CAPÍTULO VII

Comunicaciones de las Administraciones públicas

Artículo 13. *Red de comunicaciones de las Administraciones públicas españolas.*

1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, aprobado por el Consejo Superior de Administración Electrónica, para su interconexión a través de las redes de comunicaciones de las Administraciones públicas.

Artículo 15. *Hora oficial.*

1. Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen.

2. La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al Centro Español de Metrología y, cuando sea posible, con la hora oficial a nivel europeo.

CAPÍTULO VIII

Reutilización y transferencia de tecnología

Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones y de la documentación asociada, y de otros objetos de información de los cuales las Administraciones públicas sean titulares de los derechos de propiedad intelectual y que éstas puedan poner a disposición de otras Administraciones públicas y de los ciudadanos, sin contraprestación y sin necesidad de convenio, tendrán en cuenta que el fin perseguido es el aprovechamiento y la reutilización,

así como la protección contra su apropiación en exclusiva por parte de terceros, en condiciones tales que eximan de responsabilidad al cedente por el posible mal uso por parte del cesionario, así como la no obligación a la asistencia técnica o el mantenimiento por parte del cedente, ni de compensación alguna en caso de errores en la aplicación.

2. Las administraciones utilizarán para las aplicaciones que declaren como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información que se comparten:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas mismas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio de aplicaciones para su libre reutilización que podrá ser accedido a través del Centro de Transferencia de Tecnología.

2. Las Administraciones públicas enlazarán los directorios de aplicaciones para su libre reutilización a los que se refiere el artículo 46 de la Ley 11/2007, de 22 de junio, entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones públicas deberán tener en cuenta las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados.

4. Las Administraciones públicas procurarán la publicación del código de las aplicaciones, en desarrollo o finalizadas, en los directorios de aplicaciones para su libre reutilización con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia.

CAPÍTULO IX

Firma electrónica y certificados

Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

2. Las Administraciones públicas aprobarán y publicarán su política de firma electrónica y de certificados partiendo de la norma técnica establecida a tal efecto en disposición adicional primera, que podrá convivir junto con otras políticas particulares para una transacción determinada en un contexto concreto.

3. Las Administraciones públicas receptoras de documentos electrónicos firmados permitirán la validación de las firmas electrónicas contra la política de firma indicada en la firma del documento electrónico, siempre que dicha política de firma se encuentre dentro de las admitidas por cada Administración pública para el reconocimiento mutuo o multilateral con otras Administraciones públicas.

4. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa.

Dichos certificados serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos.

5. La política de firma electrónica y de certificados, mencionada en el apartado primero del presente artículo, establecerá las características técnicas y operativas de la lista de prestadores de servicios de certificación de confianza que recogerá los certificados reconocidos e interoperables entre las Administraciones públicas y que se consideren fiables para cada nivel de aseguramiento concreto, tanto en el ámbito nacional como europeo. La lista que establezca la Administración General del Estado podrá ser utilizada como referencia por otras Administraciones públicas para definir sus listas de servicios de confianza para aplicación dentro de sus ámbitos competenciales.

6. Las aplicaciones usuarias de certificados electrónicos y firma electrónica:

a) Se atendrán a la política de firma electrónica y de certificados aplicable en su ámbito en relación con los diversos aspectos contemplados y particularmente con la aplicación de los datos obligatorios y opcionales, las reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

b) Permitirán los mecanismos de acreditación y representación de los ciudadanos en materia de identificación y firma electrónica, previstos en la normativa correspondiente.

Artículo 19. *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

1. De acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, sobre obligaciones de los prestadores de servicios de certificación, en relación con la interoperabilidad, dichos prestadores cumplirán con lo indicado en los apartados siguientes.

2. En relación con la interoperabilidad organizativa, los prestadores de los servicios de certificación dispondrán de lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Establecimiento de los usos de los certificados expedidos de acuerdo con un perfil dado y sus posibles límites de uso.

b) Prácticas al generar los certificados que permitan posteriormente la aplicación de unos mecanismos de descubrimiento y extracción inequívoca de los datos de identidad del certificado.

c) Definición de la información de los certificados o relacionada con ellos que será publicada por parte del prestador, debidamente catalogada.

d) Definición de los posibles estados en los que un certificado pueda encontrarse a lo largo de su ciclo de vida.

e) Los niveles de acuerdo de servicio definidos y caracterizados para los servicios de validación y de sellado de fecha y hora.

3. En relación con la interoperabilidad semántica, los prestadores de servicios de certificación aplicarán lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) La definición de los perfiles de certificados que describirán, mediante mínimos, el contenido obligatorio y opcional de los diferentes tipos de certificados que emiten, así como la información acerca de la sintaxis y semántica de dichos contenidos.

b) Establecimiento de los campos cuya unicidad de información permitirá su uso en labores de identificación.

4. En relación con la interoperabilidad técnica, los prestadores de los servicios de certificación aplicarán lo siguiente, descrito en su Declaración de Prácticas de Certificación:

a) Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos, estado de los certificados, dispositivos seguros de creación de firma, programas controladores, dispositivos criptográficos, interfaces de programación, tarjetas criptográficas, conservación de documentación relativa a los certificados y servicios, límites de los certificados, conforme a lo establecido en el artículo 11.

b) La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores.

c) Los mecanismos de publicación y de depósito de certificados y documentación asociada admitidos entre Administraciones públicas.

Artículo 20. *Plataformas de validación de certificados electrónicos y de firma electrónica.*

1. Las plataformas de validación de certificados electrónicos y de firma electrónica proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas.

2. Proporcionarán, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes.

3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.

4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

CAPÍTULO X

Recuperación y conservación del documento electrónico

Artículo 21. *Condiciones para la recuperación y conservación de documentos.*

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.

b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.

c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.

e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.

f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.

g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Artículo 22. *Seguridad.*

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Artículo 23. *Formatos de los documentos.*

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato

correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Artículo 24. *Digitalización de documentos en soporte papel.*

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

2. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

CAPÍTULO XI

Normas de conformidad

Artículo 25. *Sedes y registros electrónicos.*

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

Artículo 26. *Ciclo de vida de servicios y sistemas.*

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

Artículo 27. *Mecanismo de control.*

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

Artículo 28. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

Actualización

Artículo 29. *Actualización permanente.*

El Esquema Nacional de Interoperabilidad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Digitalización de documentos: Tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones públicas.

f) Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones.

h) Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones públicas y por las Entidades de Derecho Público vinculadas o dependientes de aquéllas.

i) Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas.

j) Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

2. El Ministerio de la Presidencia, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, aprobará las normas

técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado para la Función Pública. Para la redacción y mantenimiento de las normas técnicas de interoperabilidad indicadas en el apartado 1 se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

3. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Inventario de procedimientos administrativos y servicios prestados: contendrá información de los procedimientos y servicios, clasificada con indicación del nivel de informatización de los mismos, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: publicará los modelos de datos de intercambio tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, junto con las definiciones y codificaciones asociadas; proporcionará funciones de repositorio, generación de formatos para procesamiento automatizado, colaboración, publicación y difusión de los modelos de datos que faciliten la interoperabilidad semántica entre las Administraciones públicas y de éstas con los ciudadanos; se enlazará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Directorio de aplicaciones para su libre reutilización: contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

Disposición adicional segunda. *Formación.*

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

Disposición adicional tercera. *Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.*

CENATIC, Fundación Pública Estatal, constituida por el Ministerio de Industria, Turismo y Comercio, a través de Red.es, podrá impulsar proyectos de software de fuentes abiertas dirigidos a la mejor implantación de las medidas de interoperabilidad contempladas en el presente real decreto y, al objeto de fomentar la reutilización y facilitar la interoperabilidad, se encargará de la puesta en valor y difusión de todas aquellas aplicaciones que sean declaradas de fuentes abiertas por las Administraciones Públicas.

Disposición adicional cuarta. *Instituto Nacional de Tecnologías de la Comunicación.*

INTECO, como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la sociedad del conocimiento, podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de interoperabilidad contempladas en el presente real decreto.

Disposición adicional quinta. *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

Disposición transitoria primera. *Adecuación de sistemas y servicios.*

Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Interoperabilidad de forma que permitan el cumplimiento de lo establecido en la Disposición final tercera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Interoperabilidad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación, que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Disposición transitoria segunda. *Uso de medios actualmente admitidos de identificación y autenticación.*

De acuerdo con lo previsto en el artículo 19 de la Ley 11/2007, de 22 de junio, y en la disposición transitoria primera del Real Decreto 1671/2009, de 6 de noviembre, se establece un plazo de adaptación de veinticuatro meses en el que se podrá seguir utilizando los medios actualmente admitidos de identificación y firma electrónica.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Familia: Se entiende por tal la agrupación de procedimientos administrativos atendiendo a criterios genéricos de similitud por razón de esquema de tramitación, documentación de entrada y salida e información, dejando al margen criterios de semejanza en la materia objeto del procedimiento, órgano competente, u otra información análoga.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructuras y servicios comunes: Instrumentos operativos que facilitan el desarrollo y despliegue de nuevos servicios, así como la interoperabilidad de los existentes, creando escenarios de relación multilateral y que satisfacen las necesidades comunes en los distintos ámbitos administrativos; son ejemplos la Red de comunicaciones de las Administraciones públicas españolas, la red transeuropea sTESTA, la plataforma de verificación de certificados electrónicos.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia,

eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

§ 9

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia

Jefatura del Estado
«BOE» núm. 109, de 7 de mayo de 2002
Última modificación: 24 de diciembre de 2008
Referencia: BOE-A-2002-8628

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico.

La actual regulación del Centro Superior de Información de la Defensa está contenida en una pluralidad de disposiciones, ninguna de ellas de rango legal, que han supuesto un esfuerzo de adecuación de sus estructuras y funcionamiento a los nuevos requerimientos de la sociedad y del Estado. Sin embargo, carecen de una regulación unitaria y sistemática y con el rango legal apropiado a la luz de la Constitución.

Sólo el estatuto de su personal fue diseñado por una norma con rango de Ley formal y desarrollado reglamentariamente.

Esta situación hace necesario abordar una nueva regulación de los servicios de inteligencia mediante una norma con rango de Ley, en la que se recojan de una forma unitaria y sistemática la naturaleza, objetivos, principios, funciones, aspectos sustanciales de su organización y régimen jurídico administrativo, así como los controles parlamentario y judicial, constituyendo éstos la esencia de su funcionamiento eficaz y transparente.

Esta Ley, inspirándose en el modelo de los países de nuestro entorno político y cultural, pretende, por tanto, dotar a los servicios de inteligencia de los instrumentos precisos para que puedan cumplir los objetivos que les asignen las disposiciones legales y reglamentarias.

Se crea el Centro Nacional de Inteligencia que sustituye al Centro Superior de Información de la Defensa y, dada la naturaleza y misiones que tendrá encomendadas, se configura como Organismo público especial de los previstos en la disposición adicional

décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

De esta forma, contará con la necesaria autonomía funcional para el cumplimiento de sus misiones, por lo que tendrá un régimen específico presupuestario, de contratación y de personal.

Respecto de este último, esta Ley contiene la habilitación necesaria para que el Gobierno pueda aprobar un estatuto, único y uniforme, para todo el personal que preste servicios en el Centro Nacional de Inteligencia, ya que, en caso contrario, dicho personal se regiría por legislaciones distintas dependiendo de su condición y relación con la Administración.

La principal misión del Centro Nacional de Inteligencia será la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

El Centro continuará adscrito al Ministerio de Defensa.

Esta adscripción adquiere un nuevo sentido a la luz de los nuevos retos que para los servicios de inteligencia se derivan de los llamados riesgos emergentes, que esta Ley afronta al definir las funciones del Centro. Sus objetivos, definidos por el Gobierno, serán aprobados anualmente por el Consejo de Ministros y se plasmarán en la Directiva de Inteligencia.

El Centro Nacional de Inteligencia funcionará bajo el principio de coordinación con los demás servicios de información del Estado español. A estos efectos, se crea la Comisión Delegada del Gobierno para Asuntos de Inteligencia, presidida por el Vicepresidente del Gobierno que designe su Presidente e integrada por el Ministro de Asuntos Exteriores, el Ministro de Defensa, el Ministro del Interior, el Ministro de Economía, el Secretario general de la Presidencia, el Secretario de Estado de Seguridad y el Secretario de Estado Director del Centro Nacional de Inteligencia.

Por primera vez, una Ley contempla de forma específica el principio del control parlamentario de las actividades del Centro Nacional de Inteligencia. Esta Ley, dentro del respeto a la autonomía parlamentaria, prevé que sea la Comisión que controla los créditos destinados a gastos reservados la que efectúe el control de las actividades del Centro, conociendo los objetivos que hayan sido aprobados por el Gobierno y un informe anual sobre el grado de cumplimiento de los mismos y de sus actividades. De acuerdo con la normativa parlamentaria, los miembros de esta Comisión son también los que conocen de los secretos oficiales.

El proyecto incluye aquellos aspectos de la regulación del Centro Nacional de Inteligencia que, conforme a la Constitución, no están reservados a Ley Orgánica. Es en la Ley Orgánica complementaria de la presente Ley donde se aborda el control previo de las actividades del Centro Nacional de Inteligencia.

Ambas Leyes deben ser interpretadas conjunta y sistemáticamente, ya que la adopción de las medidas que requieran autorización judicial previa deberá justificarse en el cumplimiento de las funciones que la presente Ley asigna al Centro Nacional de Inteligencia.

CAPÍTULO I

Disposiciones generales

Artículo 1. *El Centro Nacional de Inteligencia.*

El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

Artículo 2. *Principios.*

1. El Centro Nacional de Inteligencia se regirá por el principio de sometimiento al ordenamiento jurídico y llevará a cabo sus actividades específicas en el marco de las

habilitaciones expresamente establecidas en la presente Ley y en la Ley Orgánica 2/2002, de 7 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

2. Sin perjuicio de la protección de sus actividades, la actuación del Centro Nacional de Inteligencia será sometida a control parlamentario y judicial en los términos que esta Ley y la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia determinan.

3. En el desarrollo de sus funciones, el Centro Nacional de Inteligencia actuará bajo los principios de eficacia, especialización y coordinación, de acuerdo con los objetivos de inteligencia definidos por el Gobierno.

Artículo 3. *Programación de objetivos.*

El Gobierno determinará y aprobará anualmente los objetivos del Centro Nacional de Inteligencia mediante la Directiva de Inteligencia, que tendrá carácter secreto.

Artículo 4. *Funciones del Centro Nacional de Inteligencia.*

Para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones:

a) Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional.

b) Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población.

c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos.

d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro.

e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales.

Artículo 5. *Actividades del Centro Nacional de Inteligencia.*

1. Las actividades del Centro Nacional de Inteligencia, así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias, constituyen información clasificada, con el grado de secreto, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales o, en su caso, con el mayor nivel de clasificación que se contemple en dicha legislación y en los mencionados Acuerdos.

2. El Centro Nacional de Inteligencia mantendrá con el resto de las Administraciones públicas, cuando proceda, las relaciones de cooperación y coordinación necesarias para el mejor cumplimiento de sus misiones, de acuerdo con la legislación vigente en cada caso y preservando la protección legal de las actividades del Centro.

3. El Centro Nacional de Inteligencia podrá disponer y usar de medios y actividades bajo cobertura, pudiendo recabar de las autoridades legalmente encargadas de su expedición las identidades, matrículas y permisos reservados que resulten precisos y adecuados a las necesidades de sus misiones.

Asimismo, sus miembros dispondrán de documentación que les acredite, en caso de necesidad, como miembros del Centro, sin que ello exonere a la persona o entidad ante la que se produzca la acreditación de la obligación de guardar secreto sobre la identidad de dicho personal. Las autoridades competentes ante las que comparezcan miembros del Centro Nacional de Inteligencia, por motivos relacionados con actividades del servicio, adoptarán las medidas necesarias para asegurar la protección de los datos personales, identidad y apariencia de aquéllos.

También dispondrán de licencia de armas, en función de las necesidades del servicio, de acuerdo con la normativa vigente.

4. Los miembros del Centro Nacional de Inteligencia no tendrán la consideración de agentes de la autoridad, con excepción de aquellos que desempeñen cometidos profesionales relacionados con la protección del personal del Centro y de las instalaciones del mismo.

5. Para el cumplimiento de sus funciones, el Centro Nacional de Inteligencia podrá llevar a cabo investigaciones de seguridad sobre personas o entidades en la forma prevista en esta Ley y en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia. Para la realización de estas investigaciones podrá recabar de organismos e instituciones públicas y privadas la colaboración precisa.

CAPÍTULO II

De la organización y régimen jurídico

Artículo 6. *Comisión Delegada del Gobierno para Asuntos de Inteligencia.*

1. La Comisión Delegada del Gobierno para Asuntos de Inteligencia velará por la adecuada coordinación de todos los servicios de información e inteligencia del Estado para la formación de una comunidad de inteligencia.

2. La Comisión estará presidida por el Vicepresidente del Gobierno que designe su Presidente e integrada por los Ministros de Asuntos Exteriores, Defensa, Interior y Economía, así como por el Secretario general de la Presidencia, el Secretario de Estado de Seguridad y el Secretario de Estado Director del Centro Nacional de Inteligencia, que actuará como Secretario.

3. No obstante lo dispuesto en el apartado anterior, podrán ser convocados a las reuniones de la Comisión los titulares de aquellos otros órganos superiores y directivos de la Administración General del Estado que se estime conveniente.

4. Corresponde a la Comisión Delegada:

a) Proponer al Presidente del Gobierno los objetivos anuales del Centro Nacional de Inteligencia que han de integrar la Directiva de Inteligencia.

b) Realizar el seguimiento y evaluación del desarrollo de los objetivos del Centro Nacional de Inteligencia.

c) Velar por la coordinación del Centro Nacional de Inteligencia, de los servicios de información de los Cuerpos y Fuerzas de Seguridad del Estado y los órganos de la Administración civil y militar.

Artículo 7. *Organización.*

1. El Centro Nacional de Inteligencia se adscribe orgánicamente al Ministerio de Defensa.

2. Su organización, régimen económico-presupuestario y de personal se desarrollará en régimen de autonomía funcional bajo la figura de Organismo público con personalidad jurídica propia y plena capacidad de obrar.

3. El Centro Nacional de Inteligencia se estructura en una Dirección, cuyo titular tendrá rango de Secretario de Estado, una Secretaría General y en las unidades que se determinen reglamentariamente.

Artículo 8. *Régimen jurídico.*

1. El personal que preste servicios en el Centro Nacional de Inteligencia, cualquiera que sea su procedencia, estará sometido a un mismo y único estatuto de personal que será aprobado por el Gobierno y en el que, de acuerdo con las funciones y naturaleza propias del Centro, se regularán, al menos, los siguientes extremos:

a) El proceso de selección del personal, que exigirá la superación de pruebas objetivas de acuerdo con los principios de mérito y capacidad.

b) El carácter temporal o permanente de la relación de servicios con el Centro Nacional de Inteligencia.

c) La estructura jerárquica del Centro Nacional de Inteligencia y las relaciones orgánicas y funcionales consiguientes.

d) Las medidas administrativas que garanticen la reserva sobre los aspectos de gestión de personal que afecten al funcionamiento del Centro.

No obstante lo anterior, el Centro podrá contratar otro personal con carácter laboral para atender sus necesidades de mantenimiento y funcionamiento no vinculadas con el ejercicio efectivo de las funciones que la presente Ley le encomiende. Este personal podrá ser sometido a las medidas de seguridad y control que se estimen necesarias de las que se prevean con carácter general en el estatuto del personal del Centro.

e) Los supuestos, las condiciones y los efectos en que el personal del Centro pueda pasar a desempeñar puestos de trabajo en las Administraciones Públicas, con reincorporación o no a su cuerpo o escala de procedencia en los casos que así corresponda.

f) El régimen de derechos y deberes que conjugará el de la función pública y el del personal sujeto a disciplina militar.

2. El Centro Nacional de Inteligencia elaborará anualmente un anteproyecto de presupuesto y lo elevará al Ministro de Defensa para remisión al Consejo de Ministros, que lo integrará en los Presupuestos Generales del Estado para su posterior remisión a las Cortes Generales.

3. El control de la gestión económico-financiera se efectuará con arreglo a lo dispuesto en la Ley General Presupuestaria para los Organismos públicos previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. El Gobierno establecerá las peculiaridades necesarias que garanticen su autonomía e independencia funcional.

4. En su régimen patrimonial y de contratación podrá someterse al derecho privado.

5. Se autoriza al Centro Nacional de Inteligencia a disponer del 18 por 100 del total de los créditos del capítulo destinado a gastos corrientes en bienes y servicios de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija, al objeto de poder atender los gastos periódicos o repetitivos de material no inventariable, mantenimiento y conservación, tracto sucesivo, indemnizaciones por razón del servicio y otros de similares características.

6. Se autoriza al Centro Nacional de Inteligencia a disponer del 2,5 por ciento del total de los créditos del capítulo de inversiones reales de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija para las adquisiciones de material y servicios complementarios en el exterior.

Artículo 9. *Secretario de Estado Director del Centro Nacional de Inteligencia.*

1. El Secretario de Estado Director del Centro Nacional de Inteligencia será nombrado por Real Decreto a propuesta del Ministro de Defensa. El mandato será de cinco años, sin perjuicio de la facultad del Consejo de Ministros de proceder a su sustitución en cualquier momento.

2. Corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno, asegurar la adecuación de las actividades del Centro a dichos objetivos y ostentar la representación de aquél.

Asimismo, le corresponde:

a) Elaborar la propuesta de estructura orgánica del Centro Nacional de Inteligencia y nombrar y separar a los titulares de sus órganos directivos.

b) Aprobar el anteproyecto de presupuesto.

c) Mantener los procedimientos de relación necesarios para el desarrollo de las actividades específicas del Centro Nacional de Inteligencia, así como la celebración de los contratos y convenios con entidades públicas o privadas que sean precisos para el cumplimiento de sus fines.

d) Mantener y desarrollar, dentro del ámbito de su competencia, la colaboración con los servicios de información de las Fuerzas y Cuerpos de Seguridad del Estado, y los órganos de la Administración civil y militar, relevantes para los objetivos de inteligencia.

e) Ejercer las facultades que otorgue la legislación vigente a los Presidentes y Directores de Organismos públicos y las que les atribuyan las disposiciones de desarrollo.

f) Desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional.

g) Realizar cuantas otras funciones le sean atribuidas legal o reglamentariamente.

Artículo 10. *Secretario general del Centro Nacional de Inteligencia.*

1. El Secretario general del Centro Nacional de Inteligencia, con rango de Subsecretario, será nombrado por Real Decreto a propuesta del Ministro de Defensa, entre personas de reconocida experiencia y competencia profesional en el ámbito de la Inteligencia. Sustituirá al Director en los casos de ausencia, vacante o enfermedad.

2. El Secretario general del Centro Nacional de Inteligencia ejercerá las funciones que le otorgue el Real Decreto de estructura del Centro, y, en particular, las siguientes:

a) Apoyar y asistir al Director del Centro Nacional de Inteligencia en el ejercicio de sus funciones.

b) Establecer los mecanismos y sistemas de organización del Centro y determinar las actuaciones precisas para su actualización y mejora.

c) Dirigir el funcionamiento de los servicios comunes del Centro a través de las correspondientes instrucciones y órdenes de servicio.

d) Desempeñar la jefatura superior del personal del Centro, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

e) Las demás que legal o reglamentariamente se le encomienden.

CAPÍTULO III

Del control

Artículo 11. *Control parlamentario.*

1. El Centro Nacional de Inteligencia someterá al conocimiento del Congreso de los Diputados, en la forma prevista por su Reglamento, a través de la Comisión que controla los créditos destinados a gastos reservados, presidida por el Presidente de la Cámara, la información apropiada sobre su funcionamiento y actividades. El contenido de dichas sesiones y sus deliberaciones será secreto.

2. La citada Comisión del Congreso de los Diputados tendrá acceso al conocimiento de las materias clasificadas, con excepción de las relativas a las fuentes y medios del Centro Nacional de Inteligencia y a aquellas que procedan de servicios extranjeros u organizaciones internacionales en los términos establecidos en los correspondientes acuerdos y convenios de intercambio de la información clasificada.

3. Los miembros de la Comisión correspondiente estarán obligados, en los términos del Reglamento del Congreso de los Diputados, a guardar secreto sobre las informaciones y documentos que reciban. Una vez examinados los documentos, serán reintegrados al Centro Nacional de Inteligencia para su debida custodia, sin que se puedan retener originales, copias o reproducciones.

4. La Comisión a que se refiere este artículo conocerá de los objetivos de inteligencia establecidos anualmente por el Gobierno y del informe que, también con carácter anual,

elaborará el Director del Centro Nacional de Inteligencia de evaluación de actividades, situación y grado de cumplimiento de los objetivos señalados para el período anterior.

Artículo 12. *Control judicial previo.*

El control judicial previo del Centro Nacional de Inteligencia se llevará a cabo en la forma prevista en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia, complementaria de la presente Ley.

Disposición adicional primera. *Naturaleza jurídica.*

El Centro Nacional de Inteligencia queda incluido dentro de los Organismos públicos a que se refiere la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

Disposición adicional segunda. *Supresión del Centro Superior de Información de la Defensa.*

1. Queda suprimido el Centro Superior de Información de la Defensa.
2. El Centro Nacional de Inteligencia sucederá al Centro Superior de Información de la Defensa en el ejercicio de sus funciones y cometidos, quedando subrogado en la titularidad de los bienes, derechos y obligaciones del Estado afectos o constituidos en virtud de las mencionadas funciones y de su fondo documental.
3. Todas las referencias que contengan las disposiciones normativas vigentes al Centro Superior de Información de la Defensa, se entenderán hechas al Centro Nacional de Inteligencia.

Disposición adicional tercera. *Habilitación de adscripción orgánica.*

Se autoriza al Presidente del Gobierno para modificar, por Real Decreto, la adscripción orgánica del Centro Nacional de Inteligencia, prevista en el artículo 7.1 de esta Ley. El Departamento al que se adscriba el Centro ejercerá las competencias que, en relación con el mismo, atribuye esta Ley al Ministerio de Defensa y a su titular.

Disposición transitoria única. *Garantía de derechos adquiridos.*

1. El personal que, a la entrada en vigor de la presente Ley, tenga la consideración de personal estatutario permanente o temporal del Centro Superior de Información de la Defensa, quedará integrado en la misma condición en el Centro Nacional de Inteligencia.
2. En tanto no se produzca el desarrollo reglamentario de esta Ley y se apruebe un estatuto de personal del Centro Nacional de Inteligencia, continuará en vigor el Real Decreto 1324/1995, de 28 de julio, por el que se establece el estatuto de personal del Centro Superior de Información de la Defensa.
3. El grupo de clasificación, grado personal y demás derechos económicos que el personal del Centro Superior de Información de la Defensa tuviera reconocidos, quedarán plenamente garantizados en el nuevo régimen de personal.

Disposición derogatoria única.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente Ley.

Disposición final primera. *Facultad de desarrollo.*

Se faculta al Consejo de Ministros para dictar cuantas disposiciones sean necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Modificaciones presupuestarias.*

El Ministerio de Hacienda realizará las modificaciones presupuestarias oportunas para dar cumplimiento a lo dispuesto en la presente Ley.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor el mismo día de su publicación en el "Boletín Oficial del Estado".

§ 10

Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia

Jefatura del Estado
«BOE» núm. 109, de 7 de mayo de 2002
Última modificación: sin modificaciones
Referencia: BOE-A-2002-8627

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

EXPOSICIÓN DE MOTIVOS

La presente Ley Orgánica es complementaria de la Ley 11/2002, de 7 de mayo, reguladora del Centro Nacional de Inteligencia, y modifica la Ley Orgánica del Poder Judicial, a los efectos de establecer un control judicial de las actividades del citado Centro que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución española.

Para las actividades que puedan afectar a la inviolabilidad del domicilio y al secreto de las comunicaciones, la Constitución española exige en su artículo 18 autorización judicial, y el artículo 8 del Convenio Europeo para Protección de los Derechos Humanos y de las Libertades Fundamentales exige que esta injerencia esté prevista en la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

A estos efectos, esta Ley Orgánica, cuyo alcance resulta de una interpretación conjunta con la Ley reguladora del Centro Nacional de Inteligencia, determina tanto la forma de nombramiento de un Magistrado del Tribunal Supremo específicamente encargado del control judicial de las actividades del Centro Nacional de Inteligencia, como el procedimiento conforme al cual se acordará o no la autorización judicial necesaria para dichas actividades. El plazo para acordarlas será ordinariamente de setenta y dos horas, pudiendo reducirse, de forma extraordinaria y por motivos de urgencia debidamente justificados, a veinticuatro horas.

Artículo único. *Control judicial previo del Centro Nacional de Inteligencia.*

1. El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro.

2. La solicitud de autorización se formulará mediante escrito que contendrá los siguientes extremos:

a) Especificación de las medidas que se solicitan.

b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas.

c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse.

d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad.

3. El Magistrado acordará, mediante resolución motivada en el plazo improrrogable de setenta y dos horas, la concesión o no de la autorización solicitada. Dicho plazo se reducirá a veinticuatro horas, por motivos de urgencia debidamente justificados en la solicitud de autorización del Secretario de Estado Director del Centro Nacional de Inteligencia que, en todo caso, contendrá los extremos especificados en el apartado anterior de este artículo.

El Magistrado dispondrá lo procedente para salvaguardar la reserva de sus actuaciones, que tendrán la clasificación de secreto.

4. El Secretario de Estado Director del Centro Nacional de Inteligencia ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma.

Disposición adicional única. *Modificación de la Ley Orgánica del Poder Judicial.*

1. Se modifica el artículo 125 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

> «125. El Presidente del Consejo General del Poder Judicial tendrá las siguientes funciones:
>
> 1. Ostentar la representación del Consejo General del Poder Judicial.
> 2. Convocar y presidir las sesiones del Pleno y de la Comisión Permanente, decidiendo los empates con voto de calidad.
> 3. Fijar el orden del día de las sesiones del Pleno y de la Comisión Permanente.
> 4. Someter cuantas propuestas considere oportunas en materias de la competencia del Pleno o de la Comisión Permanente.
> 5. Someter al Pleno las propuestas de nombramiento de los Magistrados del Tribunal Supremo a que se refiere el artículo 127.4) de esta Ley.
> 6. Proponer el nombramiento de Ponencias para preparar la resolución o despacho de un asunto.
> 7. Autorizar con su firma los acuerdos del Pleno y de la Comisión Permanente.
> 8. Ejercer la superior dirección de las actividades de los órganos técnicos del Consejo.
> 9. Las demás previstas en la Ley.»

2. Se modifica el artículo 127 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

> «127. Será de la competencia del Pleno del Consejo General del Poder Judicial:

1. La propuesta de nombramiento por mayoría de 3/5 del Presidente del Tribunal Supremo y del Consejo General del Poder Judicial y del Vicepresidente de este último.

2. La propuesta de nombramiento de miembros del Tribunal Constitucional, que habrá de ser adoptada por mayoría de 3/5 de sus miembros.

3. La propuesta de nombramiento de Presidentes de Sala y Magistrados del Tribunal Supremo y cualesquiera otros discrecionales.

4. La propuesta de nombramiento del Magistrado de la Sala Segunda de lo Penal o Tercera de lo Contencioso-Administrativo, del Tribunal Supremo, competente para conocer de la autorización de las actividades del Centro Nacional de Inteligencia que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución, así como la propuesta de nombramiento del Magistrado de dichas Salas del Tribunal Supremo que lo sustituya en caso de vacancia, ausencia o imposibilidad.

5. La propuesta de nombramiento de Presidente de los Tribunales Superiores de Justicia de las Comunidades Autónomas.

6. Evacuar la audiencia prevista en el artículo 124.4 de la Constitución sobre nombramiento del Fiscal General del Estado.

7. Resolver los recursos de alzada interpuestos contra los acuerdos de la Comisión Permanente, de la Comisión Disciplinaria y de las Salas de Gobierno de los Tribunales Superiores de Justicia y de los órganos de gobierno de los Tribunales y Juzgados.

8. Resolver los expedientes de rehabilitación instruidos por la Comisión Disciplinaria.

9. Evacuar los informes previstos en la Ley y ejercer la potestad reglamentaria atribuida por la Ley al Consejo General del Poder Judicial.

10. Acordar, en los casos legalmente establecidos, la separación y jubilación de los Jueces y Magistrados en los supuestos no previstos en el artículo 131.3.

11. Elegir y nombrar los Vocales componentes de las Comisiones y Delegaciones.

12. Aprobar la memoria anual que con motivo de la apertura del año judicial leerá su Presidente sobre el estado de la Administración de Justicia.

13. Elaborar el Presupuesto del Consejo General del Poder Judicial que se integrará en los Generales del Estado, en una sección independiente.

14. Dirigir la ejecución del presupuesto del Consejo y controlar su cumplimiento.

15. Cualesquiera otras funciones que correspondan al Consejo General del Poder Judicial y no se hallen expresamente atribuidas a otros órganos del mismo.»

3. Se modifica el artículo 135 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

«135. Corresponderá a la Comisión de calificación informar, en todo caso, sobre los nombramientos de la competencia del Pleno, excepto el nombramiento del Magistrado del Tribunal Supremo previsto en el artículo 127.4) de esta Ley.»

4. Se añade un nuevo artículo 342 bis a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

«Artículo 342 bis.

El Magistrado del Tribunal Supremo competente para conocer de la autorización de las actividades del Centro Nacional de Inteligencia que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución se nombrará por un período de cinco años, a propuesta del Consejo General del Poder Judicial, entre Magistrados de dicho Tribunal que cuenten con tres años de servicios en la categoría.»

Disposición final única. *Entrada en vigor.*

La presente Ley Orgánica entrará en vigor el mismo día de su publicación en el «Boletín Oficial del Estado».

§ 11

Ley 9/1968, de 5 de abril, sobre secretos oficiales

Jefatura del Estado
«BOE» núm. 84, de 6 de abril de 1968
Última modificación: 11 de octubre de 1978
Referencia: BOE-A-1968-444

Es principio general, aun cuando no esté expresamente declarado en nuestras Leyes Fundamentales, la publicidad de la actividad de los Órganos del Estado, porque las cosas públicas que a todos interesan pueden y deben ser conocidas de todos.

Este principio de publicidad en mayor o menor extensión, se halla regulado en lo que concierne a los debates e interpelaciones en las Cortes Españolas y al despacho de los asuntos judiciales, pero, en cambio, sólo de una manera fraccionada tiene su regulación, en lo que atañe a la Administración del Estado, en dispersas disposiciones, entre las que, por su reciente promulgación, pueden citarse la Ley de Prensa (artículo séptimo) y Decreto setecientos cincuenta/mil novecientos sesenta y seis, de treinta y uno de marzo, en las que sólo se contempla la publicidad en el aspecto parcial de la información debida a las publicaciones periódicas y agencias de información. Una regulación suficiente existe en la esfera de la Administración Local.

Mas si la publicidad ha de ser característica de la actuación de los Órganos del Estado, es innegable la necesidad de imponer limitaciones, cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional.

Destancan por su especial importancia aquellas cuestiones cuyo conocimiento por personas no autorizadas pueda dañar o ponga en riesgo la seguridad del Estado o los intereses fundamentales de la Nación y que constituyen los verdaderos «secretos oficiales», protegidos por sanciones penales que, tanto en el Código Penal Común como en el de Justicia Militar, alcanzan penas de la máxima severidad. Pero esta sanción penal, especialmente represiva, sólo de una manera indirecta, por medio de la intimidación, protege el descubrimiento o revelación de secretos. Las medidas de protección eficaces son las que la propia Administración ha de establecer para garantizar que los documentos o materiales en que físicamente se reflejan los secretos, no puedan ser conocidos más que por aquellas personas que, por razón de su cometido, estén autorizadas para ello.

En este aspecto existe una laguna en nuestra legislación, que, al contrario de lo que ocurre en los Estados caracterizados por la mayor libertad de información, no prevé una regulación de las medidas protectoras de los secretos oficiales Para remediar esta situación, la Ley establece un conjunto de medidas positivas para evitar que trascienda el conocimiento de lo que debe permanecer secreto, señalando normas severas que impidan la generalización de calificaciones que tienen carácter excepcional.

Con la denominación de «materias clasificadas» también utilizada en otros países, se comprenden los dos grados de secretos oficiales generalmente admitidos. La determinación

de las Autoridades y funcionarios que pueden otorgar y levantar las calificaciones, los efectos de cada una de éstas y las líneas generales de las medidas protectoras que habrán de desarrollarse reglamentariamente y con carácter uniforme por todos los servicios afectados, constituyen el contenido fundamental de la Ley, que se completa con un sistema de protección, así como la referencia de las responsabilidades que procedan por infracciones en materia de secretos oficiales.

Asimismo, desde el punto de vista de la seguridad jurídica y de la garantía de los ciudadanos, es importante resaltar que la Ley establece la necesidad de notificar a los medios de información la declaración de «materia clasificada» cuando se prevea que ésta puede llegar a conocimiento de ellos, así como la circunstancia de que conste el hecho de la clasificación para que recaiga sobre los particulares la obligación de colaboración que impone el artículo nueve, uno. Y, en fin, se consagra la expresa admisión de recurso contencioso-administrativo contra las resoluciones sancionadoras que pongan fin a la vía administrativa, sin olvidar por lo demás el importante juego del control político que en esta materia se reconoce a las Cortes Españolas y al Consejo Nacional del Movimiento.

En su virtud, y de conformidad con la Ley aprobada por las Cortes Españolas, vengo en sancionar:

Artículo primero.

Uno. Los Órganos del Estado estarán sometidos en su actividad al principio de publicidad, de acuerdo con las normas que rijan su actuación, salvo los casos en que por la naturaleza de la materia sea ésta declarada expresamente «clasificada», cuyo secreto o limitado conocimiento queda amparado por la presente Ley.

Dos. Tendrán carácter secreto, sin necesidad de previa clasificación, las materias así declaradas por Ley.

Artículo segundo.

A los efectos de esta Ley podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado.

Artículo tercero.

Las «materias clasificadas» serán calificadas en las categorías de secreto y reservado en atención al grado de protección que requieran.

Artículo cuarto.

La calificación a que se refiere el artículo anterior corresponderá exclusivamente, en la esfera de su competencia, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor.

Artículo quinto.

La facultad de calificación a que se refiere el artículo anterior no podrá ser transferida ni delegada.

Artículo sexto.

El personal de la Administración del Estado o de las Fuerzas Armadas que tenga conocimiento de cualquier asunto que, a su juicio, reúna las condiciones del artículo segundo, deberá hacerlo llegar a alguno de los órganos comprendidos en el artículo cuarto en la forma que reglamentariamente se determine.

Artículo séptimo.

La cancelación de cualquiera de las calificaciones previstas en el artículo tercero de esta Ley será dispuesta por el órgano que hizo la respectiva declaración.

Artículo octavo.

Las calificaciones de secreto o reservado, hechas con arreglo a los términos de la presente Ley y de las disposiciones que reglamentariamente se dicten para su aplicación, determinarán, entre otros, los siguientes efectos:

A) Solamente podrán tener conocimiento de las "materias clasificadas" los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.

B) La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las «materias clasificadas».

C) El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las «materias clasificadas».

Artículo noveno.

Uno. La persona a cuyo conocimiento o poder llegue cualquier «materia clasificada», conforme a esta Ley, siempre que le conste esta condición, está obligada a mantener el secreto y entregarla a la Autoridad civil o militar más cercana y, si ello no fuese posible, a poner en conocimiento de ésta su descubrimiento o hallazgo. Esta Autoridad lo comunicará sin dilación al Departamento ministerial que estime interesado o a la Presidencia del Gobierno, adoptando entretanto las medidas de protección que su buen juicio le aconseje.

Dos. Cuando una «materia clasificada» permita prever que pueda llegar a conocimiento de los medios de información, se notificará a éstos la calificación de secreto o reservado.

Artículo diez.

Uno. Las calificaciones a que se refiere el artículo cuarto, en cualquiera de sus grados, se conferirán mediante un acto formal y con los requisitos y materializaciones que reglamentariamente se determinen.

Dos. La declaración de "materias clasificadas" no afectará al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma que determinen los respectivos Reglamentos y, en su caso, en sesiones secretas.

Tres. Las «materias clasificadas» llevarán consigo una anotación en la que conste esta circunstancia y la calificación que les corresponda conforme al artículo tercero.

Cuatro. Las copias o duplicados de una «materia clasificada» tendrán el mismo tratamiento y garantía que el original y sólo se obtendrán previa autorización especial y bajo numeración.

Artículo once.

Uno. Las personas facultadas para tener acceso a una «materia clasificada» quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen, así como las particulares que para cada caso concreto puedan establecerse.

Dos. Corresponde a los órganos señalados en el artículo cuarto conceder en sus respectivas dependencias las autorizaciones para el acceso a las "materias clasificadas", así como para su desplazamiento fuera de las mismas.

Tres. A toda persona que tenga acceso a una «materia clasificada» se le hará saber la índole de la misma con las prevenciones oportunas.

Artículo doce.

Los órganos referidos en el artículo cuarto atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de cuanto se dispone en la presente Ley y en especial por la correcta aplicación de las calificaciones de secreto o reservado y porque se promuevan las acciones penales, las medidas disciplinarias y los expedientes administrativos para corregir las infracciones a esta Ley.

Artículo trece.

Las actividades reservadas por declaración de Ley y las "materias clasificadas" no podrán ser comunicadas, difundidas ni publicadas, ni utilizado su contenido fuera de los límites establecidos por la Ley. El incumplimiento de esta limitación será sancionado, si procediere, conforme a las Leyes penales, y por vía disciplinaria, en su caso, considerándose en este último supuesto la infracción como falta muy grave.

Artículo catorce.

La calificación de secreto o reservado no impedirá el exacto cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los interesados, sin perjuicio de la eventual aplicación de las sanciones previstas en esta Ley en caso de violación del secreto por parte de los interesados.

DISPOSICIÓN FINAL

En Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarios para la aplicación de la presente Ley y protección de las «materias clasificadas».

Se determinará igualmente con todo el detalle necesario y con especificación de las medidas técnicas precisas el régimen de custodia, traslado, registro, archivo, examen y destrucción de las materias clasificadas, así como la elaboración de copias o duplicados de tales materias.

También se dispondrá lo necesario para que el personal de la Administración Civil del Estado y de las Fuerzas Armadas se halle debidamente instruido en cuestiones de seguridad y protección de secretos.

§ 12

Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales

Presidencia del Gobierno
«BOE» núm. 47, de 24 de febrero de 1969
Última modificación: sin modificaciones
Referencia: BOE-A-1969-263

La disposición final de la Ley nueve/mil novecientos sesenta y ocho, de cinco de abril, dispone que en el Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armardas, se regularán los procedimientos y medidas necesarias para la aplicación de la Ley y protección de las «materias clasificadas».

Para lograr una unificación normativa internacional y tener el mismo grado de protección a las materias clasificadas en los distintos países parece aconsejable utilizar las enseñanzas del derecho comparado, en especial el de las naciones muy industrializadas con mayor experiencia en la información tecnológica.

De acuerdo con la expresada tendencia se ha recogido en este Reglamento lo relativo a definiciones, materias clasificadas, violaciones de su protección, Servicio de Protección de Materias Clasificadas y otros particulares necesarios para la adecuada aplicación de la Ley antes mencionada.

En su virtud, a propuesta del Vicepresidente del Gobierno, de conformidad con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día cinco de febrero de mil novecientos sesenta y nueve.

DISPONGO:

Artículo primero.

De acuerdo con lo dispuesto en el artículo primero de la Ley nueve/mil novecientos sesenta y ocho, de cinco de abril, los Órganos del Estado estarán sometidos en el ejercicio de su actividad al principio de publicidad, salvo en las materias que tengan por Ley el carácter de secretas o en aquellas otras que, por su naturaleza, sean expresamente declaradas como «clasificadas».

Artículo segundo. *Definiciones.*

A efectos de lo dispuesto en el artículo segundo de la Ley podrá entenderse:

Uno. Por asuntos, todos los temas que se refieran a las materias que en el mismo se especifican.

Dos. Por acto, cualquier manifestación o acuerdo de la vida político-administrativa tendente a la obtención de fines específicos.

Tres. Por documentos, cualquier constancia gráfica o de cualquier otra naturaleza y muy especialmente:

a) Los impresos, manuscritos, papeles mecanografiados o taquigrafiados y las copias de los mismos, cualesquiera sean los procedimientos empleados para su reproducción: los planos, proyectos, esquemas, esbozos, diseños, bocetos, diagramas, cartas, croquis y mapas de cualquier índole, ya lo sean en su totalidad, ya las partes o fragmentos de los mismos.

b) Las fotografías y sus negativos, las diapositivas, los positivos y negativos de película, impresionable por medio de cámaras cinematográficas y sus reproducciones.

c) Las grabaciones sonoras de todas clases.

d) Las planchas, moldes, matrices, composiciones tipográficas, piedras litográficas, grabados en película cinematográfica, bandas escritas o perforadas, la memoria transitorizada de un cerebro electrónico y cualquier otro material usado para reproducir documentos.

Cuatro. Por informaciones, los conocimientos de cualquier clase de asuntos o los comprendidos como materias clasificadas en el citado artículo segundo de la Ley.

Cinco. Por datos y objetos, los antecedentes necesarios para el conocimiento completo o Incompleto de las materias clasificadas, las patentes, las materias primas y los productos elaborados, el utillaje, cuños, matrices y sellos de todas clases, así como los lugares, obras, edificios e Instalaciones de interés para la defensa nacional o la investigación científica.

Seis. Se entenderá también como materias propias de este Decreto, todas aquellas que, sin estar enumeradas en el presente artículo, por su naturaleza, puedan ser calificadas de asunto, acto, documento, información, dato u objeto, de acuerdo con lo dispuesto en el artículo dos de la Ley.

Artículo tercero. *Materias clasificadas de «secreto» y de «reservado».*

I. La clasificación de «secreto» se aplicará a todas las materias referidas en el artículo anterior que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado, o pudiera comprometer los Intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.

II. La clasificación de «reservado» se aplicará a tos asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a los referidos intereses fundamentales de la Nación, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

III. Siempre que ello sea posible, la autoridad encargada de la calificación indicará el plazo de duración de ésta, con mención de si pudiera ser suprimida o rebajada de grado. Para ello, podrá fijar una fecha o indicar un acontecimiento o hecho límite de dicho plazo. Tal indicación no deberá incluirse en el texto, sino que constará en una anotación, anterior o posterior, al mismo.

De la misma manera, la citada Autoridad, en el momento de verificar la clasificación, señalará del personal a sus órdenes, aquellos que puedan tener acceso a las materias «secretas» o «reservadas», indicando, en cada caso, las formalidades y limitaciones que sean necesarias para el cumplimiento de esta clasificación.

IV. A efectos de evitar la acumulación excesiva de material calificado, la autoridad encargada de la calificación deberá señalar los procedimientos para determinar, periódicamente, la conveniencia de la reclasificación o desclasificación de aquel material.

Artículo cuarto. *Violaciones de la protección de las materias clasificadas.*

Cualquier persona que preste sus servicios en la Administración del Estado o en las Fuerzas Armadas, sea cual fuere su situación, que tenga conocimiento de cualquier asunto que, a su juicio, reúna las condiciones de «secreto» o «reservado», o conozca de la revelación a persona no autorizada de materias clasificadas, o compruebe el extravío de cualquier documento o material clasificado, deberá poner estos hechos, inmediatamente, en

conocimiento de su Jefe inmediato. Este Jefe, siguiendo el proceso reglamentario más rápido, lo pondrá, igualmente, en conocimiento del Jefe del Servicio de Protección de Materias Clasificadas del Ministerio en el cual preste sus servicios, en su defecto, del Director general o autoridad equivalente del Organismo al cual la materia de referencia estuviera confiada o de aquel a quien afectare la revelación de información o el extravío del documento o material de referencia.

Artículo quinto.

Si en un Organismo, Entidad o Servicio, sea Autoridad encargada de hacer la calificación, sea depositario de materias clasificadas, se comprobase una revelación no autorizada o el extravío de documentos o material, la máxima jerarquía de aquéllos deberá ordenar se proceda, con carácter de máxima urgencia, a hacer las averiguaciones pertinentes, tanto para fijar las responsabilidades a que hubiere lugar, que habrán de atribuirse, siempre que sea posible, a persona determinada individualmente y no al cargo o función que desempeñare, como para la recuperación del documento o material extraviado.

Artículo sexto.

Si el extravío, o la revelación de información, correspondiese a una materia con la calificación de «secreto», el Director general o autoridad equivalente, comunicará, inmediatamente, tal hecho al Servicio de Protección de Materias Clasificadas del Ministerio correspondiente.

Si se tratase de una materia con calificación de «reservado», deberá ordenar se proceda a registrar su falta en el archivo o depósito correspondiente, si lo hubiere, y a adoptar las medidas pertinentes para su recuperación y esclarecimiento

Artículo séptimo.

La apreciación y decisión con carácter definitivo, en relación con las actuaciones investigadoras referidas en el artículo quinto, corresponderán, en todo caso, y oído el Servicio de Protección de Materias Clasificadas correspondiente, al Ministro del Departamento de que se trate.

Artículo octavo.

En caso de extravío de documentación o material, y si fuere encontrada la materia clasificada, el Director general o autoridad equivalente, deberá comunicar tal hecho al Servicio de Protección de Materias Clasificadas aportando tanto los datos suficientes que permitan su correcta identificación, cuanto los pormenores relativos a la circunstancia del hallazgo.

Artículo noveno. *Servicio de Protección de Materias Clasificadas.*

Los Servicios de Protección de Materias Clasificadas de los Departamentos ministeriales, que tendrán la consideración de Unidades Centrales en aquellos casos en que así se precise, o de Dependencias afectas directamente al despacho de los Ministros respectivos y que estarán a cargo de funcionarios de su libre designación, deberán:

a) Asegurar el adecuado tratamiento de las materias clasificadas, tanto si se han producido en el Departamento como si se han recibido en el mismo procedentes de otras dependencias de la Administración.

b) Instruir convenientemente respecto de las normas de protección al personal que tenga acceso, fehacientemente autorizado, al material clasificado,

c) Elaborar las condiciones de seguridad privativas del Ministerio, de las cuales deberán tener constancia, junto con las disposiciones necesarias para asegurar el perfecto cumplimiento de lo establecido en este Decreto, las Entidades y personas del propio Ministerio con competencia para la declaración de materias clasificables, según se dispone en el artículo cuarto de la Ley.

d) Responder en todo tiempo, de la mejor protección del material calificado que se le entregue para su custodia y, especialmente, de cerrar bajo seguro el material calificado de

«secreto» en instalación de seguridad apropiada, siempre que la misma no esté en uso o bajo supervisión directa de funcionarios autorizados.

e) Establecer procedimientos adecuados tendentes a evitar que personas no autorizadas puedan tener acceso, sea visual, sea auditivo, a información o material secreto, no discutiéndose con o en presencia de personas no autorizadas, el contenido de aquéllos.

f) Mantener el control o registro de las materias clasificadas.

Artículo diez. *Funcionarios del Servicio de Protección de Materias Clasificadas.*

El cumplimiento de las medidas de protección deberá constituir parte principal de la tarea o función de cada uno de los funcionarios adscritos a los Servicios de Protección de Materias Clasificadas y no un cometido accesorio.

Artículo once. *Requisitos formales de la clasificación.*

El acto formal de clasificación habrá de ajustarse a los siguientes requisitos:

A) Si se trata de calificación otorgada por autoridades legitimadas para ello por el número uno del artículo cuarto de la Ley, en el documento origen de aquélla deberá hacerse constar la autoridad que la atribuya, la declaración constitutiva de materia clasificada, el ámbito a que se refiere según se dispone en el artículo segundo de la Ley, el lugar, fecha, sello y firma entera o abreviada de aquélla. Una diligencia se adherirá a la materia clasificada, la cual comprenderá todos los aspectos que dicho documento comprende.

B) En el caso de tratarse de la clasificación provisional a que se refiere el número dos del referido artículo cuarto de la Ley, la autoridad que la proponga deberá especificar los mismos requisitos anteriores y añadirá una explicación razonada del porqué de la misma. Dentro del plazo legal al efecto establecido, la autoridad competente, según lo dispuesto en el número uno del artículo de referencia, antes de proceder a la firma o aprobación de la calificación propuesta, comprobara si su contenido corresponde con las definiciones establecidas en los párrafos I y II del artículo tercero de este Decreto, con especificación de los requisitos señalados en el párrafo anterior. Caso de no existir justificación, promoverán que dicha calificación provisional sea disminuida o desechada.

C) En el caso de que partes destacadas de documentos o material exijan la calificación de secreto, y existan otras a las cuales pudiera corresponder calificación inferior, cada una de dichas partes será clasificada de acuerdo con su contenido, pero el documento o material en su conjunto, ostentará la calificación más elevada, haciéndose constar así en el documento que atribuya la calificación.

D) Si tales documentos o material son trasladados a Entidades u Organismos distintos del de origen, aparte los datos anteriores, deberán especificar en la notificación escrita de la calificación atribuida lo siguiente: «Este material contiene información relativa a secretos oficiales, según lo dispuesto en la Ley nueve/mil novecientos sesenta y ocho de cinco de abril».

E) La información de defensa de naturaleza reservada, suministrada a España por un país extranjero o por una Organización internacional, recibirá una clasificación que asegure un grado de protección equivalente o mayor que el requerido por el Gobierno u Organismo internacional que suministró la información.

F) La notificación de la calificación a que se refiere el número dos del artículo noveno de la Ley se efectuará por conducto del Director general de Prensa, en la forma establecida en la Ley de Procedimiento Administrativo.

Artículo doce. *Lugares para la custodia y salvaguardia del material clasificado.*

La posesión o uso de información o material clasificado como secreto estará limitada a lugares donde se disponga de instalaciones para su almacenaje y segura protección, y a los cuales no pueden tener acceso otras personas que no sean las que, de manera fehaciente, hayan sido autorizadas para ello por las autoridades señaladas en el artículo cuarto de la Ley.

Artículo trece. *Custodia del material clasificado como «secreto».*

Por lo menos, los documentos, información y material clasificado de «secreto», estará guardado en una caja fuerte o armario-archivador a prueba de incendios y dotados de cerraduras de combinación de disco, cuyas dimensiones, peso, construcción e instalación hagan mínimas las posibilidades de robo, violación e indiscreciones.

De ser ello necesario, por el volumen total del material clasificado, podrán habilitarse salas o sótanos aprobados al efecto por la persona responsable del Servicio de Protección de Materias Clasificadas que impliquen unas condiciones, cuando menos, similares a los sistemas indicados en el apartado anterior.

Si no fuere posible disponer de las instalaciones especificadas en los párrafos anteriores, las materias clasificadas de «secreto» deberán estar protegidas por una guardia armada.

Artículo catorce. *Custodia del material clasificado como «reservado».*

Como mínimo, los documentos, información y material clasificados de «reservado» deberán ser almacenados en la forma especificada para los clasificados de «secreto» o en armarios-archivadores metálicos y equipados con barras de cierre en acero, con candado cambiable, tipo combinación, o en otras instalaciones que garanticen unas condiciones de seguridad semejantes.

Artículo quince. *Cambio de combinaciones de cerraduras.*

Las combinaciones de las cerraduras de los equipos de seguridad sólo podrán ser cambiadas por personas que tengan el adecuado visado de seguridad y en los casos siguientes:

A) Que una persona conocedora de la combinación sea trasladada de la dependencia a que pertenece el equipo, o se la haya retirado el visado o credencial de seguridad.

B) Que la combinación haya sido sometida a reparación.

C) Siempre que el Jefe del Servicio de Protección de Materias Clasificadas lo estime oportuno, de acuerdo con el Ministro.

D) Como mínimo una vez al año.

Artículo dieciséis. *Marcas en documentos encuadernados, no encuadernados y en planos, croquis y otros documentos reservados.*

La clasificación asignada a documentos encuadernados, tales como libros o folletos cuyas páginas estén sólida y permanentemente unidas, deberá estar visiblemente marcada o estampillada en el exterior de la cubierta frontal, en la página del titulo, en la primera página, en la última página y en el exterior de la cubierta posterior. En cada caso, las marcas se estamparan en la parte superior e inferior de la página o cubierta.

Si se tratase de documentos no encuadernados, tales como escritos, cartas, memorandums, informes, telegramas y otros documentos similares, cuyas páginas no están unidas de manera sólida y permanente, las marcas o estampillas deberán hacerse en la parte superior e inferior de cada página, de forma que la señal quede claramente visible cuando las paginas estén grapadas o sujetas con clips.

En el caso de planos, mapas, croquis, bocetos y demás documentos similares, la marca de clasificación se estampara bajo la leyenda, cuerpo o título o escala, de tal forma que quede claramente reproducida en todas las copias que de los mismos se obtengan. Dicha clasificación deberá ser marcada también en la parte superior e inferior en cada caso.

Artículo diecisiete. *Sustitución de funciones.*

Cuando la persona a cuya custodia estuvieren confiadas materias clasificadas fuere sustituida en las funciones que ejerciera, se ausentare por un periodo superior a quince días, o por cualquier otro motivo, no pudiere continuar ejerciendo tal encargo, deberá proceder a hacer entrega de aquéllos a persona reglamentariamente designada para sustituirla, mediante la elaboración de un inventario que deberá estar conformado por el funcionario entrante y el saliente.

Esta formalidad deberá cumplimentarse antes de que la persona a sustituir haya cesado de forma reglamentaria en el cargo.

Artículo dieciocho. *Traslado del material «secreto».*

El traslado fuera de los lugares específicamente destinados a la custodia de material clasificado como «secreto» se llevará a cabo de la siguiente forma:

Se hará cubierta interior y exterior opacas. La cubierta interior será lacrada y con sello de seguridad, con la indicación de «secreto», la dirección a donde aquel se transmite y con la indicación de que sólo podrá ser abierta por su destinatario.

En la cubierta exterior, también debidamente lacrada, sólo figurará la dirección correspondiente, sin ningún índice de la clasificación de su contenido.

Adjunto a la cubierta interior llevará un impreso de recepción o «recibo» que identificará al remitente, destinatario y documento o material, sin contener ninguna indicación secreta y que deberá devolverse firmado y sellado por el receptor.

Artículo diecinueve. *Traslado del material «reservado».*

Si se tratase de material clasificado de «reservado», su traslado deberá llevarse a cabo también en dos cubiertas, de las cuales la exterior no llevará ninguna clasificación de seguridad. La interior, precintada y sellada, con la Indicación escueta de la clasificación y la dirección a donde aquél se transmite.

En este caso, sólo se requerirá un recibí si el expedidor lo juzga necesario.

Artículo veinte. *Transmisión del material «secreto».*

La transmisión de material secreto se llevará a cabo, preferiblemente, por medio de contacto directo de los funcionarios a quienes tal función corresponda, o por personal específicamente designado, valija diplomática, por un sistema de correos creado expresamente para este fin o por medios de transmisión en forma cifrada.

Artículo veintiuno. *Transmisión del material «reservado».*

La de material reservado se llevará a cabo de la misma manera que la expuesta para el secreto en el articulo anterior o por medio de los comandantes de aeronaves o navíos con categoría de oficial o correo certificado si no fuere practicable ninguno de los procedimientos anteriores, cifrándose los textos siempre que sea posible.

Artículo veintidós. *Transmisión dentro del órgano de origen.*

Si la transmisión de material clasificado se llevase a cabo dentro del órgano de origen, se regirá por las normas que elabore el Servicio de Protección de Materias Clasificadas correspondiente, las cuales deberán garantizar un grado de seguridad equivalente al indicado para transmisión fuera del mismo.

Artículo veintitrés. *Control de transmisión.*

En todo tiempo se mantendrá un control adecuado de la transmisión de material clasificado, llevándose un registro contable exacto del material transmitido, con una severa limitación del número de documentos entregados y copias que de los mismos se hagan.

Artículo veinticuatro. *Prohibición de la información por teléfono.*

La información clasificada no podrá ser transmitida o revelada por medio del teléfono, excepto en los casos en que así se disponga, expresamente, por medio de determinados circuitos, tanto civiles como militares.

Artículo veinticinco. *Registro de material clasificado.*

La persona responsable del Servicio de Protección de Materias Clasificadas supervisará el registro de todo el material clasificado en un Impreso especial, en el cual figurarán el órgano de origen, la fecha y la calificación correspondiente; el movimiento de tal material y

su destrucción, en su caso. Cada impreso especial deberá referirse a una materia, pudiéndose agrupar en un solo legajo todo el material que se refiera al mismo concepto.

Todos los ejemplares de un documento clasificado serán numerados por la Autoridad encargada de la calificación, y lo mismo deberá hacerse cuando una entidad distinta fuere autorizada para su reproducción. En este caso, la Autoridad encargada de calificar indicará los números correspondientes a los ejemplares de copia.

A continuación del número de ejemplares deberá figurar el número de folios del mismo.

Artículo veintiséis. *Inventario del material clasificado.*

En todos los Servicios de Protección de Materias Clasificadas, la persona responsable de los mismos procederá a realizar un inventario en el mes de enero de cada año. De su resultado se remitirá certificación al Ministro del Departamento, quien la devolverá con su conformidad o reparos.

Artículo veintisiete. *Examen del material clasificado.*

El examen de materias clasificadas sólo se autorizará mediante expedición de la correspondiente autorización por la Autoridad encargada de la calificación, a personas cuyos deberes oficiales requieren tal acceso, y con especificación de si se trata de una sola vez o con carácter habitual y ello, únicamente, si han sido calificadas en aquella autorización como personal de confianza.

En todo caso, en el Servicio de Protección de Materias Clasificadas se llevará un registro contable de las personas a las cuales se haya facilitado acceso al material clasificado, incorporándose un ejemplar, de un documento debidamente firmado por el Jefe del Servicio y la persona autorizada, al legajo correspondiente con especificación de las circunstancias personales, fecha. Autoridad que extendió la autorización y contenido de ésta.

Por otra parte, y a menos que en la autorización se disponga expresamente lo contrario, no se permitirá, en ningún caso, la toma de notas, datos y demás pormenores del material correspondiente.

La persona responsable del Servicio, por sí o por medio de otra persona a sus órdenes, y de cuya actuación sea aquélla responsable, deberá estar presente en todo momento, mientras dure el examen del material.

Artículo veintiocho. *Destrucción de material clasificado.*

Siempre que la Autoridad encargada de la calificación juzgare que el material clasificado resultare ya inservible, ordenará su destrucción a todas las dependencias que lo poseyeren o hubiesen obtenido copias o reproducciones del mismo.

Nadie podrá, en circunstancias normales, destruir material clasificado sin haber obtenido, previamente, autorización de aquella Autoridad.

Si algún Organismo, luego de haber recibido orden de destrucción de determinado material clasificado, entendiese que algún ejemplar continúa siendo necesario, solicitará, motivadamente, de la Autoridad calificadora, la correspondiente autorización para conservarlo.

Artículo veintinueve. *Procedimientos de destrucción y destrucción de emergencia del material clasificado.*

El material clasificado será destruido por medio del fuego, procedimientos químicos o, cuando tales medios no existan, por medio de artefactos que los reduzcan a pulpa o fragmentos tan minúsculos que imposibiliten su reconstrucción.

En todo caso, la destrucción habrá de ser completa.

Artículo treinta.

La destrucción deberá llevarse a cabo bajo la supervisión de la persona responsable del Servicio de Protección de Materias Clasificadas, debiendo ser certificada por el mismo y dándose cuenta inmediatamente de ello, por conducto reglamentario, a la autoridad calificadora.

Dichos certificados de destrucción serán numerados dentro de cada año por el Organismo interesado. En la hoja de control del Organismo que procedió a la distribución del material o autorizó su destrucción deberá cumplimentarse el espacio referente a la recepción de los certificados.

Artículo treinta y uno.

Todos los Organismos poseedores de material clasificado deberán tener previsto, para casos de emergencia, un plan de destrucción del conjunto de aquél.

Dicho plan deberá ser estudiado por la persona responsable del Servicio de Protección de Materias Clasificadas, la cual, a la vista de los sistemas más accesibles y adecuados, deberá adoptar las medidas necesarias para su inmediata y rápida ejecución.

Artículo treinta y dos.

Cualquier persona que tuviere a su cargo la elaboración o copia de material clasificable, deberá adoptar las medidas tendentes a que sean destruidos, en el más breve plazo posible, los borradores, minutas, hojas inutilizadas y papeles químicos u otros elementos que hayan servido para tales fines.

Artículo treinta y tres. *Programas de entrenamiento y ordenación.*

Las personas responsables de los Servicios de Protección de Materias Clasificadas establecerán y mantendrán programas activos de entrenamiento y orientación para loe funcionarios que en ellos presten sus servicios, a fin de inculcarles el sentido de la responsabilidad personal que, a cada uno, incumbe, en orden a proceder, en todo momento, con especial vigilancia y cuidado, al cumplimiento de las órdenes que reciba y a la más estricta observancia de las medidas de protección vigentes.

Como mínimo, dichos programas habrán de comprender:

A) Precisa explicación y análisis de las medidas de protección.

B) Formas de llevar a cabo su más exacto cumplimiento.

C) Identificación de personas y comprobación de autorizaciones de acceso a las materias clasificadas.

D) Las normas sobre utilización, conservación y destrucción cuando fueren pertinentes y oportunas.

E) Medidas correspondientes antes y durante el traslado o transmisión del material clasificado.

F) Cualesquiera otras que tiendan a la mejor consecución de los fines perseguidos.

Artículo treinta y cuatro. *Calificación de las faltas disciplinarias y administrativas.*

La difusión o publicación de las actividades reservadas por declaración de Ley, o de «materias clasificadas», tanto por parte del personal adscrito a los Servicios de Protección de Materias Clasificadas, cuanto por cualesquiera otras personas al servicio de la Administración, aparte la responsabilidad penal que, en su caso, produjeren, tendrán la consideración, a efectos disciplinarios y administrativos, de faltas muy graves.

En las restantes violaciones de las normas contenidas en este Decreto, la gravedad de la falta será determinada por la naturaleza de la infracción y por las posibles consecuencias que de ella pudieran derivarse.

Artículo treinta y cinco.

De conformidad con lo dispuesto en el artículo catorce de la Ley, la calificación de secreto o reservado no impedirá el exacto cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los Interesados, en la forma establecida en la Ley de Procedimiento Administrativo, sin perjuicio de la eventual aplicación de las sanciones previstas en caso de violación del secreto por parte de los interesados.

Disposición adicional.

De acuerdo con lo establecido en los artículos nueve, apartado C), y once, apartado E), del presente Decreto, y teniendo en cuenta las especiales características de todo orden que concurren en el normal desenvolvimiento de la función que a las Fuerzas Armadas atribuye la Ley Orgánica del Estado, los Departamentos ministeriales correspondientes, sin perjuicio de lo dispuesto con carácter general en este Decreto, podrán elaborar normas específicas de régimen Interior para el mejor cumplimiento de la alta misión que, por precepto legal, les está encomendada.

De la misma manera y en atención a las peculiares características del servicio diplomático y a las circunstancias en que éste desarrolla sus funciones fuera del territorio nacional, el Ministerio de Asuntos Exteriores podrá elaborar también normas específicas de régimen interior para sus oficinas en el extranjero, sin perjuicio de las normas de carácter general contenidas en el presente Decreto.

§ 13

Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 1981
Última modificación: sin modificaciones
Referencia: BOE-A-1981-12774

DON JUAN CARLOS I, REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica:

CAPÍTULO PRIMERO

Disposiciones comunes a los tres estados

Artículo primero.

Uno. Procederá la declaración de los estados de alarma, excepción o sitio cuando circunstancias extraordinarias hiciesen imposible el mantenimiento de la normalidad mediante los poderes ordinarios de las Autoridades competentes.

Dos. Las medidas a adoptar en los estados de alarma, excepción y sitio, así como la duración de los mismos, serán en cualquier caso las estrictamente indispensables para asegurar el restablecimiento de la normalidad. Su aplicación se realizará de forma proporcionada a las circunstancias.

Tres. Finalizada la vigencia de los estados de alarma, excepción y sitio decaerán en su eficacia cuantas competencias en materia sancionadora y en orden a actuaciones preventivas correspondan a las Autoridades competentes, así como las concretas medidas adoptadas en base a éstas, salvo las que consistiesen en sanciones firmes.

Cuatro. La declaración de los estados de alarma, excepción y sitio no interrumpe el normal funcionamiento de los poderes constitucionales del Estado.

Artículo segundo.

La declaración de los estados de alarma, excepción o sitio será publicada de inmediato en el «Boletín Oficial del Estado», y difundida obligatoriamente por todos los medios de comunicación públicos y por los privados que se determinen, y entrará en vigor desde el instante mismo de su publicación en aquél. También serán de difusión obligatoria las disposiciones que la Autoridad competente dicte durante la vigencia de cada uno de dichos estados.

Artículo tercero.

Uno. Los actos y disposiciones de la Administración Pública adoptados durante la vigencia de los estados de alarma, excepción y sitio serán impugnables en vía jurisdiccional de conformidad con lo dispuesto en las leyes.

Dos. Quienes como consecuencia de la aplicación de los actos y disposiciones adoptadas durante la vigencia de estos estados sufran, de forma directa, o en su persona, derechos o bienes, daños o perjuicios por actos que no les sean imputables, tendrán derecho a ser indemnizados de acuerdo con lo dispuesto en las leyes.

CAPÍTULO II

El estado de alarma

Artículo cuarto.

El Gobierno, en uso de las facultades que le otorga el artículo ciento dieciséis, dos, de la Constitución podrá declarar el estado de alarma, en todo o parte del territorio nacional, cuando se produzca alguna de las siguientes alteraciones graves de la normalidad.

a) Catástrofes, calamidades o desgracias públicas, tales como terremotos, inundaciones, incendios urbanos y forestales o accidentes de gran magnitud.

b) Crisis sanitarias, tales como epidemias y situaciones de contaminación graves.

c) Paralización de servicios públicos esenciales para la comunidad, cuando no se garantice lo dispuesto en los artículos veintiocho, dos, y treinta y siete, dos, de la Constitución, concurra alguna de las demás circunstancia o situaciones contenidas en este artículo.

d) Situaciones de desabastecimiento de productos de primera necesidad.

Artículo quinto.

Cuando los supuestos a que se refiere el artículo anterior afecten exclusivamente a todo, o parte del ámbito territorial de una Comunidad Autónoma, el Presidente de la misma, podrá solicitar del Gobierno la declaración de estado de alarma.

Artículo sexto.

Uno. La declaración del estado de alarma se llevará a cabo mediante decreto acordado en Consejo de Ministros.

Dos. En el decreto se determinará el ámbito territorial, la duración y los efectos del estado de alarma, que no podrá exceder de quince días. Sólo se podrá prorrogar con autorización expresa del Congreso de los Diputados, que en este caso podrá establecer el alcance y las condiciones vigentes durante la prórroga.

Artículo séptimo.

A los efectos del estado de alarma la Autoridad competente será el Gobierno o, por delegación de éste, el Presidente de la Comunidad Autónoma cuando la declaración afecte exclusivamente a todo o parte del territorio de una Comunidad.

Artículo octavo.

Uno. El Gobierno dará cuenta al Congreso de los Diputados de la declaración del estado de alarma y le suministrará la información que le sea requerida.

Dos. El Gobierno también dará cuenta al Congreso de los Diputados de los decretos que dicte durante la vigencia del estado de alarma en relación con éste.

Artículo noveno.

Uno. Por la declaración del estado de alarma todas las Autoridades civiles de la Administración Pública del territorio afectado por la declaración, los integrantes de los

Cuerpos de Policía de las Comunidades Autónomas y de las Corporaciones Locales, y los demás funcionarios y trabajadores al servicio de las mismas, quedarán bajo las órdenes directas de la Autoridad competente en cuanto sea necesaria para la protección de personas, bienes y lugares, pudiendo imponerles servicios extraordinarios por su duración o por su naturaleza.

Dos. Cuando la Autoridad competente sea el Presidente de una Comunidad Autónoma podrá requerir la colaboración de los Cuerpos y Fuerzas de Seguridad del Estado, que actuarán bajo la dirección de sus mandos naturales.

Artículo diez.

Uno. El incumplimiento o la resistencia a las órdenes de la Autoridad competente en el estado de alarma será sancionado con arreglo a lo dispuesto en las leyes.

Dos. Si estos actos fuesen cometidos por funcionarios, las Autoridades podrán suspenderlos de inmediato en el ejercicio de sus cargos, pasando, en su caso, el tanto de culpa al juez, y se notificará al superior jerárquico, a los efectos del oportuno expediente disciplinario.

Tres. Si fuesen cometidos por Autoridades, las facultades de éstas que fuesen necesarias para el cumplimiento de las medidas acordadas en ejecución de la declaración de estado de alarma podrán ser asumidas por la Autoridad competente durante su vigencia.

Artículo once.

Con independencia de lo dispuesto en el artículo anterior, el decreto de declaración del estado de alarma, o los sucesivos que durante su vigencia se dicten, podrán acordar las medidas siguientes:

a) Limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, o condicionarlas al cumplimiento de ciertos requisitos.

b) Practicar requisas temporales de todo tipo de bienes e imponer prestaciones personales obligatorias.

c) Intervenir y ocupar transitoriamente industrias, fábricas, talleres, explotaciones o locales de cualquier naturaleza, con excepción de domicilios privados, dando cuenta de ello a los Ministerios interesados.

d) Limitar o racionar el uso de servicios o el consumo de artículos de primera necesidad.

e) Impartir las órdenes necesarias para asegurar el abastecimiento de los mercados y el funcionamiento de los servicios de los centros de producción afectados por el apartado d) del artículo cuarto.

Artículo doce.

Uno. En los supuestos previstos en los apartados a) y b) del artículo cuarto, la Autoridad competente podrá adoptar por sí, según los casos, además de las medidas previstas en los artículos anteriores, las establecidas en las normas para la lucha contra las enfermedades infecciosas, la protección del medio ambiente, en materia de aguas y sobre incendios forestales.

Dos. En los casos previstos en los apartados c) y d) del artículo cuarto el Gobierno podrá acordar la intervención de empresas o servicios, así como la movilización de su personal, con el fin de asegurar su funcionamiento. Será de aplicación al personal movilizado la normativa vigente sobre movilización que, en todo caso, será supletoria respecto de lo dispuesto en el presente artículo.

CAPÍTULO III

El estado de excepción

Artículo trece.

Uno. Cuando el libre ejercicio de los derechos y libertades de los ciudadanos, el normal funcionamiento de las instituciones democráticas, el de los servicios públicos esenciales

para la comunidad, o cualquier otro aspecto del orden público, resulten tan gravemente alterados que el ejercicio de las potestades ordinarias fuera insuficiente para restablecerlo y mantenerlo, el Gobierno, de acuerdo con el apartado tres del artículo ciento dieciséis de la Constitución, podrá solicitar del Congreso de los Diputados autorización para declarar el estado de excepción.

Dos. A los anteriores efectos, el Gobierno remitirá al Congreso de los Diputados una solicitud de autorización que deberá contener los siguientes extremos:

a) Determinación de los efectos del estado de excepción, con mención expresa de los derechos cuya suspensión se solicita, que no podrán ser otros que los enumerados en el apartado uno del artículo cincuenta y cinco de la Constitución.

b) Relación de las medidas a adoptar referidas a los derechos cuya suspensión específicamente se solicita.

c) Ambito territorial del estado de excepción, así como duración del mismo, que no podrá exceder de treinta días.

d) La cuantía máxima de las sanciones pecuniarias que la Autoridad gubernativa esté autorizada para imponer, en su caso, a quienes contravengan las disposiciones que dicte durante el estado de excepción.

Tres. El Congreso debatirá la solicitud de autorización remitida por el Gobierno, pudiendo aprobarla en sus propios términos o introducir modificaciones en la misma.

Artículo catorce.

El Gobierno, obtenida la autorización a que hace referencia el artículo anterior, procederá a declarar el estado de excepción, acordando para ello en Consejo de Ministros un decreto con el contenido autorizado por el Congreso de los Diputados.

Artículo quince.

Uno. Si durante el estado de excepción, el Gobierno considerase conveniente la adopción de medidas distintas de las previstas en el decreto que lo declaró, procederá a solicitar del Congreso de los Diputados la autorización necesaria para la modificación del mismo, para lo que se utilizará el procedimiento, que se establece en los artículos anteriores.

Dos. El Gobierno, mediante decreto acordado en Consejo de Ministros, podrá poner fin al estado de excepción antes de que finalice el período para el que fue declarado, dando cuenta de ello inmediatamente al Congreso de los Diputados.

Tres. Si persistieran las circunstancias que dieron lugar a la declaración del estado de excepción, el Gobierno podrá solicitar del Congreso de los Diputados la prórroga de aquél, que no podrá exceder de treinta días.

Artículo dieciséis.

Uno. La Autoridad gubernativa podrá detener a cualquier persona si lo considera necesario para la conservación del orden, siempre que, cuando menos, existan fundadas sospechas de que dicha persona vaya a provocar alteraciones del orden público. La detención no podrá exceder de diez días y los detenidos disfrutarán de los derechos que les reconoce el artículo diecisiete, tres, de la Constitución.

Dos. La detención habrá de ser comunicada al juez competente en el plazo de veinticuatro horas. Durante la detención, el Juez podrá, en todo momento, requerir información y conocer personalmente, o mediante delegación en el Juez de Instrucción del partido o demarcación donde se encuentre el detenido la situación de éste.

Artículo diecisiete.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, dos, de la Constitución, la Autoridad gubernativa podrá disponer inspecciones, registros domiciliarios si lo considera necesario para el esclarecimiento de los hechos presuntamente delictivos o para el mantenimiento del orden publico.

Dos. La inspección o el registro se llevarán a cabo por la propia Autoridad o por sus agentes, a los que proveerá de orden formal y escrita.

Tres. El reconocimiento de la casa, papeles y efectos, podrá ser presenciado por el titular o encargado de la misma o por uno o más individuos de su familia mayores de edad y, en todo caso, por dos vecinos de la casa o de las inmediaciones, si en ellas los hubiere, o, en su defecto, por dos vecinos del mismo pueblo o del pueblo o pueblos limítrofes.

Cuatro. No hallándose en ella al titular o encargado de la casa ni a ningún individuo de la familia, se hará el reconocimiento en presencia únicamente de los dos vecinos indicados.

Cinco. La asistencia de los vecinos requeridos para presenciar el registro será obligatoria y coercitivamente exigible.

Seis. Se levantará acta de la inspección o registro, en la que se harán constar los nombres de las personas que asistieren y las circunstancias que concurriesen, así como las incidencias a que diere lugar. El acta será firmada por la autoridad o el agente que efectuare el reconocimiento y por el dueño o familiares y vecinos. Si no supieran o no quisiesen firmar se anotará también esta incidencia.

Siete. La autoridad gubernativa comunicará inmediatamente al Juez competente las inspecciones y registros efectuados, las causas que los motivaron y los resultados de los mismos, remitiéndole copia del acta levantada.

Artículo dieciocho.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, tres, de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público.

Dos. La intervención decretada será comunicada inmediatamente por escrito motivado al Juez competente.

Artículo diecinueve.

La autoridad gubernativa podrá intervenir y controlar toda clase de transportes, y la carga de los mismos.

Artículo veinte.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo diecinueve de la Constitución, la autoridad gubernativa podrá prohibir la circulación de personas y vehículos en las horas y lugares que se determine, y exigir a quienes se desplacen de un lugar a otro que acrediten su identidad, señalándoles el itinerario a seguir.

Dos. Igualmente podrá delimitar zonas de protección o seguridad y dictar las condiciones de permanencia en las mismas y prohibir en lugares determinados la presencia de persona que puedan dificultar la acción de la fuerza pública.

Tres. Cuando ello resulte necesario, la Autoridad gubernativa podrá exigir a personas determinadas que comuniquen, con una antelación de dos días, todo desplazamiento fuera de la localidad en que tengan su residencia habitual.

Cuatro. Igualmente podrá disponer su desplazamiento fuera de dicha localidad cuando lo estime necesario.

Cinco. Podrá también fijar transitoriamente la residencia de personas determinadas en localidad o territorio adecuados a sus condiciones personales.

Seis. Corresponde a la Autoridad gubernativa proveer de los recursos necesarios para el cumplimiento de las medidas previstas en este artículo y, particularmente, de las referidas a viajes, alojamiento y manutención de la persona afectada.

Siete. Para acordar las medidas a que se refieren los apartados tres, cuatro y cinco de este artículo, la Autoridad gubernativa habrá de tener fundados motivos en razón a la peligrosidad que para el mantenimiento del orden público suponga la persona afectada por tales medidas.

Artículo veintiuno.

Uno. La Autoridad gubernativa podrá suspender todo tipo de publicaciones, emisiones de radio y televisión, proyecciones, cinematográficas y representaciones teatrales, siempre y

cuando la autorización del Congreso comprenda la suspensión del artículo veinte, apartados uno, a) y d), y cinco de la Constitución. Igualmente podrá ordenar el secuestro de publicaciones.

Dos. El ejercicio de las potestades a que se refiere el apartado anterior no podrá llevar aparejado ningún tipo de censura previa.

Artículo veintidós.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo veintiuno de la Constitución, la autoridad gubernativa podrá someter a autorización previa o prohibir la celebración de reuniones y manifestaciones.

Dos. También podrá disolver las reuniones y manifestaciones a que se refiere el párrafo anterior.

Tres. Las reuniones orgánicas que los partidos políticos, los sindicatos y las asociaciones empresariales realicen en cumplimiento de los fines que respectivamente les asignen los artículos sexto y séptimo de la Constitución, y de acuerdo con sus Estatutos, no podrán ser prohibidas, disueltas ni sometidas a autorización previa.

Cuatro. Para penetrar en los locales en que tuvieran lugar las reuniones, la Autoridad gubernativa deberá proveer a sus agentes de autorización formal y escrita. Esta autorización no será necesaria cuando desde dichos locales se estuviesen produciendo alteraciones graves del orden público constitutivas del delito o agresiones a las Fuerzas de Seguridad y en cualesquiera otros casos de flagrante delito.

Artículo veintitrés.

La Autoridad gubernativa podrá prohibir las huelgas y la adopción de medidas de conflicto colectivo, cuando la autorización del Congreso comprenda la suspensión de los artículos veintiocho, dos, y treinta y siete, dos de la Constitución.

Artículo veinticuatro.

Uno. Los extranjeros que se encuentren en España vendrán obligados a realizar las comparecencias que se acuerden, a cumplir las normas que se dicten sobre renovación o control de permisos de residencia y cédulas de inscripción consular y a observar las demás formalidades que se establezcan.

Dos. Quienes contravinieren las normas o medidas que se adopten, o actuaren en connivencia con los perturbadores del orden público, podrán ser expulsados de España, salvo que sus actos presentaren indicios de ser constitutivos de delito, en cuyo caso se les someterá a los procedimientos judiciales correspondientes.

Tres. Los apátridas y refugiados respecto de los cuales no sea posible la expulsión se someterán al mismo régimen que los españoles.

Cuatro. Las medidas de expulsión deberán ir acompañadas de una previa justificación sumaria de las razones que la motivan.

Artículo veinticinco.

La autoridad gubernativa podrá proceder a la incautación de toda clase de armas, municiones o sustancias explosivas.

Artículo veintiséis.

Uno. La Autoridad gubernativa podrá ordenar la intervención de industrias o comercios que puedan motivar la alteración del orden público o coadyuvar a ella, y la suspensión temporal de las actividades de los mismos, dando cuenta a los Ministerios interesados.

Dos. Podrá, asimismo, ordenar el cierre provisional de salas de espectáculos, establecimientos de bebidas y locales de similares características.

Artículo veintisiete.

La Autoridad gubernativa podrá ordenar las medidas necesarias de vigilancia y protección de edificaciones, instalaciones, obras, servicios públicos e industrias o

explotaciones de cualquier género. A estos efectos podrá emplazar puestos armados en los lugares más apropiados para asegurar la vigilancia, sin perjuicio de lo establecido en el artículo dieciocho, uno de la Constitución.

Artículo veintiocho.

Cuando la alteración del orden público haya dado lugar a alguna de las circunstancias especificadas en el artículo cuarto coincida con ellas, el Gobierno podrá adoptar además de las medidas propias del estado de excepción, las previstas para el estado de alarma en la presente ley.

Artículo veintinueve.

Si algún funcionario o personal al servicio de una Administración pública o entidad o instituto de carácter público u oficial favoreciese con su conducta la actuación de los elementos perturbadores del orden, la Autoridad gubernativa podrá suspenderlo en el ejercicio de su cargo, pasando el tanto de culpa al Juez competente y notificándolo al superior jerárquico a los efectos del oportuno expediente disciplinario.

Artículo treinta.

Uno. Si durante el estado de excepción el Juez estimase la existencia de hechos contrarios al orden público o a la seguridad ciudadana que puedan ser constitutivos de delito, oído el Ministerio Fiscal, decretará la prisión provisional del presunto responsable, la cual mantendrá, según su arbitrio, durante dicho estado.

Dos. Los condenados en estos procedimientos quedan exceptuados de los beneficios de la remisión condicional durante la vigencia del estado de excepción.

Artículo treinta y uno.

Cuando la declaración del estado de excepción afecte exclusivamente a todo o parte del ámbito territorial de una Comunidad Autónoma, la Autoridad gubernativa podrá coordinar el ejercicio de sus competencias con el Gobierno de dicha Comunidad.

CAPÍTULO IV

El estado de sitio

Artículo treinta y dos.

Uno. Cuando se produzca o amenace producirse una insurrección o acto de fuerza contra la soberanía o independencia de España, su integridad territorial o el ordenamiento constitucional, que no pueda resolverse por otros medios, el Gobierno, de conformidad con lo dispuesto en el apartado cuatro del artículo ciento dieciséis de la Constitución, podrá proponer al Congreso de los Diputados la declaración de estado de sitio.

Dos. La correspondiente declaración determinará el ámbito territorial, duración y condiciones del estado de sitio.

Tres. La declaración podrá autorizar, además de lo previsto para los estados de alarma y excepción, la suspensión temporal de las garantías jurídicas del detenido que se reconocen en el apartado tres del artículo diecisiete de la Constitución.

Artículo treinta y tres.

Uno. En virtud de la declaración del estado de sitio, el Gobierno, que dirige la política militar y de la defensa, de acuerdo con el artículo noventa y siete de la Constitución, asumirá todas las facultades extraordinarias previstas en la misma y en la presente ley.

Dos. A efectos de lo dispuesto en el párrafo anterior, el Gobierno designará la Autoridad militar que, bajo su dirección, haya de ejecutar las medidas que procedan en el territorio a que el estado de sitio se refiera.

Artículo treinta y cuatro.

La Autoridad militar procederá a publicar y difundir los oportunos bandos, que contendrán las medidas y prevenciones necesarias, de acuerdo con la Constitución, la presente ley y las condiciones de la declaración del estado de sitio.

Artículo treinta y cinco.

En la declaración del estado de sitio el Congreso de los Diputados podrá determinar los delitos que durante su vigencia quedan sometidos a la Jurisdicción Militar.

Artículo treinta y seis.

Las Autoridades civiles continuarán en el ejercicio de las facultades que no hayan sido conferidas a la Autoridad militar de acuerdo con la presente Ley. Aquellas Autoridades darán a la militar las informaciones que ésta le solicite y cuantas noticias referentes al orden público lleguen a su conocimiento.

DISPOSICIÓN DEROGATORIA

Quedan derogados los artículos veinticinco a cincuenta y uno y disposiciones finales y transitorias de la Ley cuarenta y cinco mil novecientos cincuenta y nueve, de treinta de julio, de Orden Público, así como cuantas disposiciones se opongan a lo preceptuado en la presente Ley Orgánica.

DISPOSICIÓN FINAL

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 14

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

Jefatura del Estado
«BOE» núm. 102, de 29 de abril de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-7630

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales

infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

En esa línea, se han emprendido diversas actuaciones a nivel nacional, como la aprobación, por la Secretaría de Estado de Seguridad del Ministerio del Interior, de un primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas. Así mismo, con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas, mediante el cual se dio un impulso decisivo en dicha materia. El desarrollo y aplicación de este Acuerdo supone un avance cualitativo de primer orden para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales.

Paralelamente, existen también una serie de actuaciones desarrolladas a nivel internacional en el ámbito europeo: tras los terribles atentados de Madrid, el Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004 la Comisión adoptó una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa europeo de protección de infraestructuras críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network-CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las Comunidades Autónomas.

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente

una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

La Ley consta de 18 artículos, estructurados en 3 Títulos. El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece, finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Asimismo, la Ley consta de cuatro Disposiciones Adicionales y cinco Disposiciones Finales.

Si bien el contenido material de la Ley es eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos que integran el Sistema de Protección de Infraestructuras Críticas, así como en todo lo relativo a los diferentes planes de protección, se ha optado por dotar a esta norma de rango legal, de acuerdo con el criterio del Consejo de Estado, a fin de poder cubrir suficientemente aquellas obligaciones que la Ley impone y que requieren de una cobertura legal específica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

2. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas, según lo dispuesto en los párrafos e) y f) del artículo 2 de la misma.

Artículo 2. *Definiciones.*

A los efectos de la presente Ley, se entenderá por:

a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

f) Infraestructuras críticas europeas: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE).

g) Zona crítica: aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.

h) Criterios horizontales de criticidad: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.
2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.
3. El impacto medioambiental, degradación en el lugar y sus alrededores.
4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

i) Análisis de riesgos: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

j) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

k) Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

l) Información sensible sobre protección de infraestructuras estratégicas: los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

m) Operadores críticos: las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley.

n) Nivel de Seguridad: aquel cuya activación por el Ministerio del Interior está previsto en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

o) Catálogo Nacional de Infraestructuras Estratégicas: la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

Artículo 3. *Ámbito de aplicación.*

1. La presente Ley se aplicará a las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.

2. Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.

3. La aplicación de esta Ley se efectuará sin perjuicio de:

a) La misión y funciones del Centro Nacional de Inteligencia establecidas en su normativa específica, contando siempre con la necesaria colaboración y complementariedad con aquéllas.

b) Los criterios y disposiciones contenidos en la Ley 25/1964, de 29 de abril, sobre energía nuclear, y normas de desarrollo de la misma, y en la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear, reformada por la Ley 33/2007, de 7 de noviembre.

c) Lo previsto en el Programa Nacional de Seguridad de la Aviación Civil contemplado en la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y su normativa complementaria.

Artículo 4. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será el responsable del Catálogo Nacional de Infraestructuras Estratégicas (en adelante, el Catálogo), instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley.

2. La competencia para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas, corresponderá al Ministerio del Interior, a través de la Secretaria de Estado de Seguridad, incluidas las propuestas, en su caso, del órgano competente de las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público en relación con las infraestructuras ubicadas en su demarcación territorial.

TÍTULO II

El Sistema de Protección de Infraestructuras Críticas

Artículo 5. *Finalidad.*

1. El Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.

2. Son agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes:

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.

b) El Centro Nacional para la Protección de las Infraestructuras Críticas.

c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.

d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.

f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.

g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.

h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

i) Los operadores críticos del sector público y privado.

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales.

Para el desempeño de su cometido, el Reglamento de desarrollo de esta Ley determinará sus competencias en la materia, que ejercerá con la asistencia de los demás integrantes del Sistema y, principalmente, del Centro Nacional para la Protección de las Infraestructuras Críticas.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, el CNPIC) como órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

2. El CNPIC dependerá orgánicamente de la Secretaría de Estado de Seguridad, y sus funciones serán las que reglamentariamente se establezcan.

3. Sin perjuicio de lo dispuesto en el apartado anterior, corresponderá al CNPIC la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.

Artículo 8. *Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

1. Por cada sector estratégico, se designará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema. El nombramiento, alta o baja en éste de un ministerio u organismo con responsabilidad sobre un sector estratégico se efectuará mediante la modificación del anexo de la presente Ley.

2. Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia. Para ello, colaborarán con el Ministerio del Interior a través de la Secretaría de Estado de Seguridad.

3. Con tales objetivos, los ministerios y organismos del Sistema desempeñarán las funciones que reglamentariamente se determinen.

4. Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo de la presente Ley.

Artículo 9. *Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

1. Los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, una serie de facultades respecto de las infraestructuras críticas localizadas en su demarcación.

2. El desarrollo reglamentario de dichas facultades en todo caso incluirá la intervención, a través de las Fuerzas y Cuerpos de Seguridad, en la implantación de los diferentes Planes de Protección Específico y de Apoyo Operativo, así como la propuesta a la Secretaría de Estado de Seguridad de la declaración de una zona como crítica.

3. No obstante lo dispuesto en el apartado primero de este artículo, las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, aquellas facultades de las Delegaciones del Gobierno relativas a la coordinación de los cuerpos policiales autonómicos y, en su caso, a la activación por aquellos del Plan de Apoyo Operativo que corresponda para responder ante una alerta de seguridad.

Artículo 10. *Comunidades Autónomas y Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

2. En todo caso, las Comunidades Autónomas mencionadas en el apartado anterior participarán en el proceso de declaración de una zona como crítica, en la aprobación del Plan de Apoyo Operativo que corresponda, y en las reuniones del Grupo de Trabajo Interdepartamental. Asimismo, serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas.

3. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

Artículo 11. *Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad.

2. La Comisión será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas.

3. Sus funciones y composición serán las que reglamentariamente se establezcan.

Artículo 12. *Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Sistema contará con un Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo), cuya composición y funciones se determinarán reglamentariamente.

2. Le corresponderá, en todo caso, la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

Artículo 13. *Operadores críticos.*

1. Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.

b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo.

e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

2. Será requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.

3. La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan.

4. Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

TÍTULO III

Instrumentos y comunicación del Sistema

Artículo 14. *Instrumentos de planificación del Sistema.*

1. La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes planes de actuación:

a) El Plan Nacional de Protección de las Infraestructuras Críticas.
b) Los Planes Estratégicos Sectoriales.
c) Los Planes de Seguridad del Operador.
d) Los Planes de Protección Específicos.
e) Los Planes de Apoyo Operativo.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, elaborará el Plan Nacional de Protección de las Infraestructuras Críticas, siendo éste el documento estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha contra el terrorismo.

3. Los Planes Estratégicos Sectoriales serán asimismo elaborados por el Grupo de Trabajo y aprobados por la Comisión, e incluirán, por sectores, los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo.

4. Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

5. Los Planes de Apoyo Operativo deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención,

protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos.

6. El contenido concreto y el procedimiento de elaboración, aprobación y registro de cada uno de los planes serán los que se determinen reglamentariamente.

Artículo 15. *Seguridad de las comunicaciones.*

1. La Secretaría de Estado de Seguridad arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC, así como su difusión a los organismos autorizados.

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

Artículo 16. *El Responsable de Seguridad y Enlace.*

1. Los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca.

2. En todo caso, el Responsable de Seguridad y Enlace designado deberá contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica.

3. Las funciones específicas del Responsable de Seguridad y Enlace serán las previstas reglamentariamente.

Artículo 17. *El Delegado de Seguridad de la Infraestructura Crítica.*

1. Los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un Delegado de Seguridad para dicha infraestructura.

2. El plazo para efectuar dicha comunicación, así como las funciones específicas del Delegado de Seguridad de la Infraestructura Crítica, serán los que reglamentariamente se establezcan.

Artículo 18. *Seguridad de los datos clasificados.*

El operador crítico deberá garantizar la seguridad de los datos clasificados relativos a sus propias infraestructuras, mediante los medios de protección y los sistemas de información adecuados que reglamentariamente se determinen.

Disposición adicional primera. *Normativa y régimen económico aplicable a la Comisión Nacional para la Protección de las Infraestructuras Críticas y al Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

En lo no previsto en la presente Ley, se estará a lo dispuesto para el funcionamiento de los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Así mismo, el funcionamiento y los trabajos de la Comisión, así como del Grupo de Trabajo previstos en la presente norma se llevarán a cabo con cargo a las dotaciones presupuestarias y los medios personales y tecnológicos del Ministerio del Interior, sin que supongan incremento alguno del gasto público.

Disposición adicional segunda. *Clasificación de los Planes.*

Los Planes a los que se refiere el artículo 14 de la presente Ley tendrán la clasificación que les corresponda en virtud de la normativa vigente en la materia, la cual deberá constar de forma expresa en el instrumento de su aprobación.

Disposición adicional tercera. *Fuerzas y Cuerpos de Seguridad.*

Las referencias efectuadas en la presente Ley a las Fuerzas y Cuerpos de Seguridad incluyen, en todo caso, a los Cuerpos policiales dependientes de las Comunidades Autónomas con competencias estatutarias reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

Disposición adicional cuarta. *Ceuta y Melilla.*

De conformidad con lo establecido en los Estatutos de Autonomía de las Ciudades de Ceuta y Melilla, los Consejos de Gobierno de ambas, de acuerdo con la Delegación del Gobierno respectiva, podrán emitir informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras situadas en ellas que sean objeto de la presente Ley.

Disposición final primera. *Título competencial.*

Esta Ley se dicta al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29.ª de la Constitución Española en materia de seguridad pública.

Disposición final segunda. *Competencias en materia de Protección Civil.*

Lo dispuesto en esta Ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía.

Disposición final tercera. *Incorporación de Derecho comunitario.*

Mediante esta Ley y sus ulteriores desarrollos reglamentarios se incorpora al Derecho español la Directiva 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

1. Se habilita al Gobierno para que en plazo de seis meses dicte el Reglamento de la presente Ley.
2. Igualmente se habilita al Gobierno a modificar por Real Decreto, a propuesta del titular del Ministerio del Interior y del titular del Departamento competente por razón de la materia, el Anexo de esta Ley.
3. En el ámbito de sus competencias, las Comunidades Autónomas podrán igualmente elaborar las normas reglamentarias necesarias para el desarrollo de la presente Ley.

Disposición final quinta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Sectores estratégicos y Ministerios/Organismos del sistema competentes

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia.
	Ministerio Interior.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio.
	Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación.
	Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Ciencia e Innovación.
	Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

§ 15

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

Ministerio del Interior
«BOE» núm. 121, de 21 de mayo de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-8849

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Reglamento de ejecución de desarrollo de la mencionada Ley.

En cumplimiento de este mandato, el presente real decreto se aprueba, en primer lugar, con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, máxime cuando del tenor de la misma se desprende no sólo la articulación de un complejo Sistema de carácter interdepartamental para la protección de las infraestructuras críticas, compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado, sino el diseño de todo un planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación.

En segundo lugar, este texto normativo no sólo es coherente con el marco legal del que trae causa, sino que además sirve a los fines del Sistema Nacional de Gestión de Situaciones de Crisis y cumple con la transposición obligatoria de la Directiva 2008/114/CE, del Consejo de la Unión Europea, de 8 de diciembre, en vigor desde el 12 de enero de 2009, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. A ello obedecen las amplias previsiones que el texto contempla en el ámbito de los diferentes Planes que deben elaborar tanto las Administraciones Públicas –en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo– como las empresas, organizaciones o instituciones clasificadas como operadores críticos, a quienes la Ley asigna una serie de obligaciones, entre las que se encuentran la elaboración de sendos instrumentos de planificación: los Planes de Seguridad del Operador y los Planes de Protección Específicos.

Asimismo, la Ley prevé que los operadores críticos designen a un Responsable de Seguridad y Enlace –a quien se exige la habilitación de director de seguridad que concede el Ministerio del Interior al personal de seguridad de las empresas de Seguridad Privada en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, o habilitación equivalente, según su normativa específica–. Igualmente, se contempla la designación de un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas.

En lo que a su contenido se refiere, el presente real decreto consta de un artículo único, una disposición transitoria única y dos disposiciones finales. Por su parte, el Reglamento consta de 36 artículos estructurados en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un artículo a la figura del Catálogo Nacional de Infraestructuras Estratégicas, como instrumento de la Secretaría de Estado de Seguridad del Ministerio del Interior que debe aglutinar todos los datos y la valoración de la criticidad de las citadas infraestructuras y que será empleado como base para planificar las actuaciones necesarias en materia de seguridad y protección de las mismas, al nutrirse de las aportaciones de los propios operadores. El Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la Ley, esto es, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), la Comisión Nacional para la Protección de las Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, concretando la composición, competencias y funcionamiento de todos ellos. El Título III se encarga de la regulación de los instrumentos de planificación, centrándose en cada uno de los Planes antes citados, cuyo proceso de elaboración, aprobación y registro, así como sus contenidos materiales, regula con mayor detalle. Finalmente, el Título IV está consagrado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

La tramitación del presente real decreto ha sido fruto de un intenso diálogo y colaboración entre los distintos Departamentos Ministeriales y organismos afectados, contando también con la aportación de las distintas Comunidades Autónomas y del sector empresarial, tras el trámite de información pública otorgado a todos ellos, lo que ha contribuido a dotar al texto de un extenso y, por otro lado, imprescindible, grado de consenso.

En su virtud, a propuesta del Vicepresidente Primero del Gobierno y Ministro del Interior, con la aprobación previa del Vicepresidente Tercero del Gobierno y Ministro de Política Territorial y Administración Pública, con el informe favorable de la Vicepresidenta Segunda del Gobierno y Ministra de Economía y Hacienda, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 20 de mayo de 2011,

DISPONGO:

TÍTULO I

Artículo único. *Aprobación del Reglamento de Protección de las infraestructuras críticas.*

En desarrollo y ejecución de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se aprueba el Reglamento de Protección de las Infraestructuras Críticas, cuyo texto se inserta a continuación.

Disposición transitoria única. *Unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General.*

Las unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General del Centro Nacional para la Protección de las Infraestructuras Críticas continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios, hasta que se aprueben las relaciones de puestos de trabajo adaptadas a la estructura organizativa proyectada en el ámbito de la protección de las infraestructuras críticas. Dicha adaptación en ningún caso podrá generar incremento de gasto público.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia atribuida al Estado en materia de seguridad pública en el artículo 149.1.29.ª de la Constitución.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto y ámbito de aplicación

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto desarrollar el marco previsto en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, a fin de concretar las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) así como los diferentes instrumentos de planificación del mismo.

2. Asimismo, regula las especiales obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas, según lo dispuesto en el artículo 2, párrafos e) y f) de la citada Ley.

Artículo 2. *Ámbito de aplicación.*

El ámbito de aplicación del presente reglamento será el previsto por el artículo 3 de la Ley 8/2011, de 28 de abril.

CAPÍTULO II

El Catálogo Nacional de Infraestructuras Estratégicas

Artículo 3. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Catálogo Nacional de infraestructuras estratégicas (en adelante, el Catálogo) es el registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas así como aquéllas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE.

2. La finalidad principal del Catálogo es valorar y gestionar los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquéllas y, en caso de ser necesario, activar, conforme a lo previsto por el Plan Nacional de Protección de las Infraestructuras Críticas, una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate.

Artículo 4. *Contenido del Catálogo.*

1. En el Catálogo deberán incorporarse, entre otros datos, los relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad que precisan en función de los riesgos evaluados así como la información obtenida de las Fuerzas y Cuerpos de Seguridad.

2. El Catálogo se nutrirá de la información que le faciliten al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC) los operadores de las

infraestructuras así como el resto de sujetos responsables del Sistema relacionados en el artículo 5 de la Ley 8/2011, de 28 de abril.

3. El Catálogo Nacional de Infraestructuras Estratégicas tiene, conforme a lo dispuesto en la legislación vigente en materia de secretos oficiales, la calificación de SECRETO, conferida por Acuerdo de Consejo de Ministros de 2 de noviembre de 2007, calificación que comprende, además de los datos contenidos en el propio Catálogo, los equipos, aplicaciones informáticas y sistemas de comunicaciones inherentes al mismo, así como el nivel de habilitación de las personas que pueden acceder a la información en él contenida.

Artículo 5. *Gestión y actualización del Catálogo.*

1. La custodia, gestión y mantenimiento del Catálogo Nacional de infraestructuras estratégicas corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será responsable de clasificar una infraestructura como estratégica y, en su caso, como infraestructura crítica o infraestructura crítica europea, así como de incluirla por vez primera en el Catálogo, previa comprobación de que cumple uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) de la Ley 8/2011, de 28 de abril.

3. El proceso de identificación de una infraestructura como crítica se realizará por el CNPIC, que podrá recabar la participación y el asesoramiento del interesado, así como de los agentes del Sistema competentes, a los que informará posteriormente del resultado de tal proceso.

4. La clasificación de una infraestructura como crítica europea supondrá la obligación adicional de comunicar su identidad a otros Estados miembros que puedan verse afectados de forma significativa por aquélla, de acuerdo con lo previsto por la Directiva 2008/114/CE. En tal caso, las notificaciones, en reciprocidad con otros Estados miembros, se realizarán por el CNPIC, de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.

5. En los casos en que se produzca una modificación relevante que afecte a las infraestructuras inscritas y que sea de interés a los efectos previstos en el presente reglamento, los operadores críticos responsables de las mismas facilitarán, a través de los medios puestos a su disposición por el Ministerio del Interior, los nuevos datos de aquéllas al CNPIC, que deberá validarlos con carácter previo a su incorporación al Catálogo. En todo caso, la actualización de los datos disponibles deberá hacerse con periodicidad anual.

TÍTULO II

Los agentes del Sistema de Protección de Infraestructuras Críticas

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las Infraestructuras Críticas Nacionales, para lo cual su titular, u órgano en quien delegue, ejercerá las siguientes funciones:

a) Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas.

b) Aprobar el Plan Nacional de Protección de las Infraestructuras Críticas y dirigir su aplicación, declarando en su caso los niveles de seguridad a establecer en cada momento, conforme al contenido de dicho Plan y en coordinación con el Plan de Prevención y Protección Antiterrorista.

c) Aprobar los Planes de Seguridad de los Operadores y sus actualizaciones a propuesta del CNPIC, tomando en su caso, como referencia, las actuaciones del órgano u organismo competente para otorgar a aquéllos las autorizaciones correspondientes en virtud de su normativa sectorial.

d) Aprobar los diferentes Planes de Protección Específicos o las eventuales propuestas de mejora de éstos a propuesta del CNPIC, en los términos de lo dispuesto en el artículo 26 de este reglamento.

e) Aprobar los Planes de Apoyo Operativo, así como supervisar y coordinar la implantación de los mismos y de aquellas otras medidas de prevención y protección que deban activarse tanto por las Fuerzas y Cuerpos de Seguridad y por las Fuerzas Armadas, en su caso, como por los propios responsables de seguridad de los operadores críticos.

f) Aprobar, previo informe del CNPIC, la declaración de una zona como crítica, a propuesta de las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

g) Identificar los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; analizando los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados.

h) Emitir las instrucciones y protocolos de colaboración dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas, así como fomentar la adopción de buenas prácticas.

i) Responder del cumplimiento de las obligaciones y compromisos asumidos por España en el marco de la Directiva 2008/114/CE, sin perjuicio de las competencias que corresponden al Ministerio de Asuntos Exteriores y de Cooperación.

j) Supervisar, dentro del ámbito de aplicación de este reglamento, los proyectos y estudios de interés y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.

k) Colaborar con los Ministerios y organismos integrados en el Sistema en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril y del presente reglamento.

l) Cualesquiera otras funciones que, eventualmente, pudieran acordarse por la Comisión Delegada del Gobierno para Situaciones de Crisis.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

El CNPIC del Ministerio del Interior, orgánicamente dependiente de la Secretaría de Estado de Seguridad, tendrá el nivel orgánico que se determine en la correspondiente relación de puestos de trabajo, y desempeñará las siguientes funciones:

a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas conforme a lo previsto en el artículo 16 de este reglamento.

c) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

d) Mantener operativo y actualizado el Catálogo, estableciendo los procedimientos de alta, baja y modificación de las infraestructuras, tanto nacionales como europeas, que en él se incluyan en virtud de los criterios horizontales y de los efectos de interdependencias sectoriales a partir de la información que le suministren los operadores y el resto de agentes del Sistema, así como establecer su clasificación interna.

e) Llevar a cabo las siguientes funciones respecto a los instrumentos de planificación previstos en este reglamento:

Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos en el marco de los Planes Estratégicos Sectoriales, para su estudio y deliberación por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo y supervisar el proceso de elaboración de éstos, recomendando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.

Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Analizar los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas o infraestructuras críticas europeas de su titularidad y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente, previo informe, respectivamente, de las Delegaciones del Gobierno en las Comunidades Autónomas o de las Comunidades Autónomas que tengan competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

f) Elevar al Secretario de Estado de Seguridad, u órgano en quien delegue, las propuestas para la declaración de una zona como crítica que se efectúen.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación Antiterrorista, los informes sobre evaluación de amenazas y tipos de vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE en representación de la Secretaría de Estado de Seguridad.

Artículo 8. *Los Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

Los ministerios y organismos del Sistema a los que se refiere el artículo 8 de la Ley 8/2011, de 28 de abril tendrán las siguientes competencias:

a) Participar, a través del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, con el apoyo, en su caso, de los operadores, en la elaboración de los Planes Estratégicos Sectoriales, así como proceder a su revisión y actualización en los términos previstos en este reglamento.

b) Verificar, en el ámbito de sus competencias, el cumplimiento de los Planes Estratégicos Sectoriales y de las actuaciones derivadas de éstos, con excepción de las que se correspondan con medidas de seguridad concretas establecidas en infraestructuras específicas, o las que deban ser realizadas por otros órganos de la Administración General del Estado, conforme a su legislación específica.

c) Colaborar con la Secretaría de Estado de Seguridad tanto en la designación de los operadores críticos como en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril, así como del presente reglamento.

d) Proporcionar asesoramiento técnico a la Secretaría de Estado de Seguridad en la catalogación de las infraestructuras dentro de su sector de competencia, poniendo a disposición del CNPIC en su caso la información técnica que ayude a determinar su criticidad, para su inclusión, exclusión o modificación en el Catálogo.

e) Custodiar, en los términos de la normativa sobre materias clasificadas y secretos oficiales, la información sensible sobre protección de infraestructuras estratégicas de la que dispongan en calidad de agentes del Sistema.

f) Designar a una persona para participar en los Grupos de Trabajo Sectoriales que, eventualmente, puedan crearse en el ámbito de la protección de infraestructuras críticas.

g) Participar, a solicitud del CNPIC o por iniciativa propia, en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas relacionadas con su sector de coordinación, en los ámbitos nacional e internacional.

h) Colaborar con la Secretaría de Estado de Seguridad en las acciones derivadas del cumplimiento de la Directiva 2008/114/CE, conforme a lo dispuesto en el artículo 7, apartado l), de este reglamento.

i) Participar en el proceso de clasificación de una infraestructura como crítica, incluyendo el ejercicio de la facultad de propuesta a tal fin.

Artículo 9. *Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

Bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, respecto de las infraestructuras críticas localizadas en su territorio, las siguientes facultades:

a) Coordinar la actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante una alerta de seguridad, y velar por la aplicación del Plan Nacional de Protección de Infraestructuras Críticas en caso de activación de éste.

b) Colaborar, en función de su ámbito territorial de actuación, con otros órganos de la Administración u organismos públicos competentes conforme a su legislación específica, así como con las delegaciones territoriales de otros ministerios y organismos del Sistema en las acciones que se desarrollen para el cumplimiento de los Planes Sectoriales vigentes en materia de protección de infraestructuras críticas.

c) Participar en la implantación de los diferentes Planes de Protección Específicos en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, en los términos en los que se expresa el Capítulo IV del Título III de este reglamento.

d) Intervenir, a través del Cuerpo Policial estatal competente, y en colaboración con el responsable de seguridad de la infraestructura, en la implantación de los diferentes Planes de Apoyo Operativo en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, conforme a lo establecido en el Capítulo V del Título III de este reglamento.

e) Proponer a la Secretaría de Estado de Seguridad a través del CNPIC la declaración de zona crítica sobre la base de la existencia de varias infraestructuras críticas o infraestructuras críticas europeas en una zona geográfica continua, con el fin de lograr una protección coordinada entre los diferentes operadores titulares y las Fuerzas y Cuerpos de Seguridad.

f) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan en calidad de agentes del Sistema, en aplicación de la normativa vigente sobre materias clasificadas y secretos oficiales.

Artículo 10. *Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, las facultades previstas en los párrafos c), d, e) y f) del artículo anterior dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento.

2. En todo caso, la coordinación de las actuaciones que se lleven a cabo en materia de protección de las infraestructuras críticas entre las Fuerzas y Cuerpos de Seguridad del Estado y los Cuerpos policiales de las Comunidades Autónomas con competencias en materia de seguridad, se regirá por lo estipulado en los acuerdos de las Juntas de Seguridad correspondientes.

3. Las Comunidades Autónomas no incluidas en el apartado primero del presente artículo participarán en el Sistema y en los órganos colegiados del mismo de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

4. De acuerdo con lo dispuesto en sus Estatutos de Autonomía, las Ciudades de Ceuta y Melilla, a través de sus Consejos de Gobierno y de acuerdo con la Delegación de Gobierno respectiva, podrán emitir los oportunos informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras críticas y críticas europeas situadas en su territorio.

Artículo 11. *La Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. La Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) desempeñará las siguientes funciones:

a) Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas en el ámbito de las Administraciones públicas.

b) Promover la aplicación efectiva de las disposiciones de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas, a partir de los informes emitidos al respecto por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

c) Llevar a cabo las siguientes actuaciones a propuesta del Grupo de Trabajo:

Aprobar los Planes Estratégicos Sectoriales.

Designar a los operadores críticos.

Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

d) Impulsar aquéllas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

2. La Comisión será presidida por el Secretario de Estado de Seguridad, y sus miembros serán:

a) En representación del Ministerio del Interior:

El Director General de la Policía y de la Guardia Civil.

El Director General de Protección Civil y Emergencias.

El Director del CNPIC, que ejercerá las funciones de Secretario de la Comisión.

b) En representación del Ministerio de Defensa, el Director General de Política de Defensa.

c) En representación del Centro Nacional de Inteligencia, un Director General designado por el Secretario de Estado-Director de aquél.

d) En representación del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, su Director.

e) En representación del Consejo de Seguridad Nuclear, el Director Técnico de Protección Radiológica.

f) En representación de cada uno de los ministerios integrados en el Sistema, una persona con rango igual o superior a Director General, designada por el titular del Departamento ministerial correspondiente en razón del sector de actividad material que corresponda.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones de la Comisión un representante con voz y voto por cada una de las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público. También participará, igualmente con voz y voto, un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

En su caso, y cuando su presencia y criterio resulte imprescindible por razón de los temas a tratar, podrán ser convocados, por decisión de su presidente, organismos, expertos u otras Administraciones públicas.

4. La Comisión se reunirá al menos una vez al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno previa convocatoria de su Presidente, quien determinará el orden del día de la reunión en los términos previstos para los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La secretaría de la Comisión radicará en el Director del CNPIC.

5. La Comisión será asistida por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Artículo 12. *El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo) desempeña las siguientes funciones:

a) Elaborar, con la colaboración de los agentes del Sistema afectados y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión, conforme a lo previsto en el Título III, Capítulo II, de este reglamento.

b) Proponer a la Comisión la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

c) Proponer a la Comisión la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, supervisando, coordinando y efectuando el seguimiento de los mismos y de sus trabajos e informando oportunamente de los resultados obtenidos a la Comisión.

d) Efectuar los estudios y trabajos que, en el marco de este reglamento, le encomiende la Comisión. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

2. El Grupo de Trabajo estará presidido por el Director del CNPIC, y estará compuesto por:

a) Un representante de cada uno de los ministerios del Sistema, designados por el titular del departamento ministerial correspondiente.

b) Un representante de la Dirección Adjunta Operativa del Cuerpo Nacional de Policía, designado por el titular de ésta.

c) Un representante de la Dirección Adjunta Operativa de la Guardia Civil, designado por el titular de aquélla.

d) Un representante de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, designado por el titular de ésta.

e) Un representante del Estado Mayor Conjunto de la Defensa, designado por el Jefe del Estado Mayor de la Defensa.

f) Un representante del Centro Nacional de Inteligencia, designado por el Secretario de Estado Director de dicho Centro.

g) Un representante del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, designado por el titular del Ministerio de la Presidencia u órgano en quien delegue, a propuesta del Director del Gabinete de la Presidencia del Gobierno.

h) Un representante del Consejo de Seguridad Nuclear, designado por el Presidente de dicho organismo.

i) Un representante del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones del Grupo de Trabajo un representante, con voz y voto por cada una de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y para el mantenimiento del orden público. Asimismo, participará con voz y voto un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

Por decisión de su presidente, podrán asistir aquellas otras Administraciones Públicas, organismos o expertos cuyo asesoramiento técnico se estime preciso en razón de los temas a tratar.

4. El Grupo de Trabajo se reunirá al menos dos veces al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno a convocatoria de su Presidente, quien determinará el orden del día de la reunión. La secretaría radicará en uno de los funcionarios que prestan servicios en el CNPIC, por decisión de su Director.

5. Para el ejercicio de las competencias que este reglamento atribuye al Grupo de Trabajo, podrán constituirse otros grupos de trabajo sectoriales para los sectores o subsectores incluidos en el anexo de la Ley 8/2011, de 28 de abril, en los que podrán participar, además del CNPIC y el correspondiente ministerio u organismo del Sistema, los operadores críticos y otros agentes del Sistema.

Artículo 13. *Operadores Críticos.*

1. Los operadores críticos serán los agentes integrantes del Sistema, que, procedentes tanto del sector público como del sector privado, reúnan las condiciones establecidas en el artículo 13 de la Ley 8/2011, de 28 de abril.

2. En aplicación de lo previsto en la citada Ley, corresponde a los operadores críticos:

a) Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo. Por ello, deberán actualizar los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento o previa validación del CNPIC.

b) Colaborar, en su caso, con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.

d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.

e) Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del presente reglamento.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por la Secretaría de Estado de Seguridad, comunicando su designación a los órganos correspondientes en virtud de lo dispuesto en el artículo 35 del presente reglamento.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial, en el marco de lo establecido en el Título III de este reglamento.

Artículo 14. *Designación de los operadores críticos.*

1. Para la designación de una empresa u organismo como operador crítico, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, en aplicación de los criterios previstos en el artículo 2, apartado h), de la Ley 8/2011, de 28 de abril. En tal caso, el CNPIC, elaborará una propuesta de resolución y la notificará al titular o administrador de aquéllas.

2. La citada propuesta contendrá la intención de designar al titular o administrador de la instalación o instalaciones como operador crítico.

3. El interesado dispondrá de un plazo de quince días a contar desde el día siguiente a la recepción de la notificación para remitir al CNPIC las alegaciones que considere procedentes, transcurrido el cual la Comisión, a propuesta del Grupo de Trabajo, dictará la resolución en la que se designará, en su caso, a dicho operador, como crítico. Esta resolución podrá ser recurrida en alzada ante el Secretario de Estado de Seguridad, y, eventualmente, con posterioridad, ante la jurisdicción contencioso-administrativa, en los términos generales previstos en la legislación vigente en materia de procedimiento administrativo y del orden jurisdiccional contencioso-administrativo.

4. Las comunicaciones con el interesado tendrán en cuenta, en todo caso, la clasificación de seguridad que corresponda según la normativa vigente.

Artículo 15. *Interlocución con los operadores críticos.*

1. Los operadores críticos del Sector Privado tendrán en el CNPIC el punto directo de interlocución con la Secretaría de Estado de Seguridad en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto este reglamento.

2. En aquellos casos en que los operadores críticos del Sector Público estén vinculados o dependan de una Administración pública, el órgano de dicha Administración que ostente competencias por razón de la materia podrá constituirse en el interlocutor con el Ministerio del Interior a través del CNPIC en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto en este reglamento, debiendo comunicar dicha decisión al CNPIC.

TÍTULO III

Instrumentos de planificación

CAPÍTULO I

El Plan Nacional de Protección de las Infraestructuras Críticas

Artículo 16. *Finalidad, elaboración y contenido.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas es el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

2. El Plan Nacional de Protección de las Infraestructuras Críticas establecerá los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

3. Asimismo, el Plan preverá distintos niveles de seguridad e intervención policial, que se activarán, en cada caso, en función de los resultados de la evaluación de la amenaza y coordinadamente con el Plan de Prevención y Protección Antiterrorista en vigor, al cual deberá adaptarse.

Los distintos niveles de seguridad contendrán la adopción graduada de dispositivos y medidas de protección ante situaciones de incremento de la amenaza contra las infraestructuras estratégicas nacionales y requerirán el concurso de las Fuerzas y Cuerpos de Seguridad, las Fuerzas Armadas, en su caso, y los responsables de los organismos o titulares o gestores de las infraestructuras a proteger.

Artículo 17. *Aprobación, registro y clasificación.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será aprobado por resolución del titular de la Secretaría de Estado de Seguridad y quedará registrado en el CNPIC, sin perjuicio de que aquellos otros organismos que necesiten conocer del mismo sean autorizados para acceder a él por el Secretario de Estado de Seguridad.

2. El Plan estará clasificado conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente tal clasificación en el instrumento de su aprobación.

Artículo 18. *Revisión y actualización.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será revisado cada cinco años por la Secretaría de Estado de Seguridad.

2. La modificación de alguno de los datos o instrucciones incluidos en el Plan Nacional de Protección de las Infraestructuras Críticas obligará a la automática actualización del mismo, que se llevará a cabo por el CNPIC y requerirá la aprobación expresa del Secretario de Estado de Seguridad.

CAPÍTULO II

Los Planes Estratégicos Sectoriales

Artículo 19. *Finalidad, elaboración y contenido.*

1. Los Planes Estratégicos Sectoriales son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los sectores contemplados en el anexo de la Ley 8/2011, de 28 de abril, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.

2. El Grupo de Trabajo, coordinado por el CNPIC, elaborará con la participación y asesoramiento técnico de los operadores afectados, en su caso, un Plan Estratégico por cada uno de los sectores o subsectores de actividad que se determinen.

3. Los Planes Estratégicos Sectoriales estarán basados en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.

4. Cada Plan Estratégico Sectorial contendrá, como mínimo, los siguientes extremos:

a) Análisis de riesgos, vulnerabilidades y consecuencias a nivel global.

b) Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.

c) Propuestas de implantación de otras medidas preventivas y de mantenimiento (por ejemplo, ejercicios y simulacros, preparación e instrucción del personal, articulación de los canales de comunicación precisos, planes de evacuación o planes operativos para abordar posibles escenarios adversos).

d) Medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

5. Los Planes Estratégicos Sectoriales podrán constituirse teniendo en cuenta otros planes o programas ya existentes, creados sobre la base de su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales reúnan los extremos a los que se refiere el apartado cuarto, podrán adoptarse los mismos como Plan Estratégico Sectorial del sector o subsector correspondiente.

Artículo 20. *Aprobación, registro y clasificación.*

1. Los Planes Estratégicos Sectoriales deberán ser aprobados por la Comisión en el plazo máximo de doce meses a partir de la entrada en vigor del presente real decreto.

2. El CNPIC gestionará y custodiará un registro central de todos los Planes Estratégicos Sectoriales existentes, una vez éstos sean aprobados por la Comisión. Los ministerios y organismos del Sistema tendrán acceso a los Planes de aquellos sectores para los que sean competentes.

3. Los Planes Estratégicos Sectoriales estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.

Artículo 21. *Revisión y actualización.*

1. Los Planes Estratégicos Sectoriales deberán ser revisados cada dos años por los ministerios y organismos del Sistema.

2. La modificación de alguno de los datos incluidos en los Planes Estratégicos Sectoriales obligará a la automática actualización de éstos, que se llevará a cabo por los ministerios y organismos del Sistema que sean competentes en el sector afectado y será posteriormente aprobada por la Comisión.

CAPÍTULO III

Los Planes de Seguridad del Operador

Artículo 22. *Finalidad, elaboración y contenido.*

1. Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

2. En el plazo de seis meses a partir de la notificación de la resolución de su designación, cada operador crítico deberá haber elaborado un Plan de Seguridad del Operador y presentarlo al CNPIC, que lo evaluará y lo informará para su aprobación, si procede, por el Secretario de Estado de Seguridad u órgano en el que éste delegue.

3. Los Planes de Seguridad del Operador deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos.

4. La Secretaría de Estado de Seguridad del Ministerio del Interior, a través del CNPIC, establecerá, con la colaboración de los Ministerios del Sistema y organismos dependientes, los contenidos mínimos de los Planes de Seguridad del Operador, así como el modelo en el que basar la elaboración de éstos.

Artículo 23. *Aprobación, registro y clasificación.*

1. El Secretario de Estado de Seguridad, u órgano en el que éste delegue, previo informe del CNPIC, aprobará el Plan de Seguridad del Operador o las propuestas de mejora del mismo, notificando la resolución al interesado en el plazo máximo de dos meses.

2. Junto a la resolución de aprobación o modificación, el CNPIC, tomando en su caso como referencia las actuaciones del organismo regulador competente en virtud de la normativa sectorial aplicable, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar.

3. El CNPIC gestionará y custodiará un registro central de todos los Planes de Seguridad del Operador existentes, una vez éstos sean aprobados por el Secretario de Estado de Seguridad. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Seguridad del Operador estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los operadores críticos responsables de la elaboración de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 24. *Revisión y actualización.*

1. Los Planes de Seguridad del Operador deberán ser revisados cada dos años por los operadores críticos y aprobados por el CNPIC. Éste podrá requerir en cualquier momento información concreta sobre el estado de implantación del Plan de Seguridad del Operador.

2. La modificación de alguno de los datos incluidos en los Planes de Seguridad del Operador obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

CAPÍTULO IV

Los Planes de Protección Específicos

Artículo 25. *Finalidad, elaboración y contenido.*

1. Los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

2. En el plazo de cuatro meses a partir de la aprobación del Plan de Seguridad del Operador, cada operador crítico deberá haber elaborado un Plan de Protección Específico por cada una de sus infraestructuras críticas así consideradas por la Secretaría de Estado de Seguridad y presentarlo al CNPIC. Igual procedimiento y plazos se establecerán cuando se identifique una nueva infraestructura crítica.

3. Los Planes de Protección Específicos de las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información.

4. Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas.

5. La Secretaría de Estado de Seguridad, a través del CNPIC, establecerá los contenidos mínimos de los Planes de Protección Específicos, así como el modelo en el que fundamentar la estructura y la compleción de éstos que, en todo caso, cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador.

Artículo 26. *Aprobación, registro y clasificación.*

1. La Secretaría de Estado de Seguridad notificará al interesado, en el plazo máximo de dos meses contados a partir de la recepción, su resolución con la aprobación de los diferentes Planes de Protección Específicos o de las eventuales propuestas de mejora de éstos. Previamente, a través del CNPIC, se recabará informe preceptivo de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas o en las Ciudades con Estatuto de Autonomía en el que se considerará, en su caso, el criterio de los órganos competentes de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, así como del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. Junto a la resolución de aprobación o modificación, el CNPIC, basándose en los informes mencionados en el punto anterior, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar sobre las infraestructuras afectadas.

3. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de las Comunidades

Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean aprobados por el Secretario de Estado de Seguridad, todos los Planes de Protección Específicos de las infraestructuras críticas o infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Protección Específicos existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Protección Específicos estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración de los respectivos planes y aquellos encargados de su registro deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 27. *Revisión y actualización.*

1. Los Planes de Protección Específicos deberán ser revisados cada dos años por los operadores críticos, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, y por el CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Protección Específicos obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

Artículo 28. *Aplicación y seguimiento.*

1. Los Delegados del Gobierno en las Comunidades Autónomas velarán por la correcta ejecución de los diferentes Planes de Protección Específicos y tendrán facultades de inspección en el ámbito de la protección de infraestructuras críticas. Dichas facultades deberán desarrollarse, en su caso, de forma coordinada con las facultades inspectoras del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. En aquellas Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, las facultades de inspección serán ejercidas por sus órganos competentes, sin perjuicio de lo dispuesto en la legislación sectorial aplicable y de la necesaria coordinación con las Delegaciones del Gobierno en dichas Comunidades y los otros organismos reguladores competentes en virtud de su normativa sectorial.

3. En ejercicio de ese seguimiento, los organismos competentes podrán en todo momento requerir del responsable de las infraestructuras críticas o infraestructuras críticas europeas la situación actualizada de la implantación de las medidas propuestas en las resoluciones de aprobación o modificación de los Planes de Protección Específicos elaborados en caso de variación de las circunstancias que determinaron su adopción, o bien para adecuarlos a la normativa vigente que les afecte, dando cuenta del resultado de ello a la Secretaría de Estado de Seguridad, a través del CNPIC.

4. Las facultades de inspección en las instalaciones portuarias, así como en aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, serán establecidas de acuerdo con lo previsto en el Real Decreto 1617/2007, de 7 de diciembre.

Artículo 29. *Compatibilidad con otros planes existentes.*

1. La elaboración de los Planes de Protección Específicos para cada una de las infraestructuras críticas se efectuará sin perjuicio del obligado cumplimiento de lo exigido por el Código Técnico de la Edificación, aprobado por el Real Decreto 314/2006, de 17 de marzo, el Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia, la normativa de Seguridad Privada o cualquier otra reglamentación sectorial específica que le sea de aplicación.

2. Las instalaciones Nucleares e Instalaciones Radiactivas que se consideren críticas reguladas en el Reglamento sobre instalaciones nucleares y radiactivas, aprobado por el Real Decreto 1836/1999 de 3 de diciembre, modificado por el Real Decreto 35/2008 de 18 de enero, integrarán sus Planes de Protección Específicos en los respectivos Planes de Protección Física rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en su normativa sectorial específica, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

3. Las instalaciones portuarias, así como aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, conforme a lo dispuesto en el Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y el transporte marítimo, integrarán sus Planes de Protección Específicos en los Planes de Protección de Puertos previstos en el citado Real Decreto rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en esa norma, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

4. En el caso de aeropuertos, aeródromos e instalaciones de navegación aérea se considerarán Planes de Protección Específicos los respectivos Programas de Seguridad de los aeropuertos aprobados conforme a lo dispuesto en la Ley 21/2003, de 7 de julio, de Seguridad Aérea modificada por la Ley 1/2011, de 4 de marzo por la que se establece el Programa Estatal de Seguridad Operacional para la Aviación Civil y se modifica la Ley 21/2003, de 7 de julio de Seguridad Aérea y en el Real Decreto 550/2006, de 5 de mayo, por el que se designa la autoridad competente responsable de la coordinación y seguimiento del Programa Nacional de Seguridad para la Aviación Civil y se determina la organización y funciones del Comité Nacional de Seguridad de la Aviación Civil. No obstante, el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la Aviación Civil podrá proponer contenidos adicionales, de conformidad con lo establecido en el artículo 25, apartado quinto de este real decreto.

CAPÍTULO V

Los Planes de Apoyo Operativo

Artículo 30. *Finalidad, elaboración y contenido.*

1. Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

2. Por cada una de las infraestructuras críticas e infraestructuras críticas europeas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura.

3. Sobre la base de sus correspondientes Planes de Protección Específicos, los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación

del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

4. El CNPIC establecerá los contenidos mínimos de los Planes de Apoyo Operativo, así como el modelo en el que fundamentar la estructura y desarrollo de éstos, que se basarán en la parte que les corresponda en la información contenida en los respectivos Planes de Protección Específicos.

5. El Ministerio de Defensa podrá acceder a los Planes de Apoyo Operativo de aquellas infraestructuras críticas o infraestructuras críticas europeas que, en caso de activarse el Plan Nacional de Protección de las Infraestructuras Críticas y a los efectos de coordinar los correspondientes apoyos de las Fuerzas Armadas, se considere oportuno, previo estudio conjunto de los mencionados apoyos.

Artículo 31. *Aprobación, registro y clasificación.*

1. Los Planes de Apoyo Operativo serán validados y aprobados por la Secretaría de Estado de Seguridad, a través del CNPIC.

2. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de cada Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean validados, todos los Planes de Apoyo Operativo de las infraestructuras críticas e infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Apoyo Operativo existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

3. Los Planes de Apoyo Operativo estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración y registro de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 32. *Revisión y actualización.*

1. Los Planes de Apoyo Operativo deberán ser revisados cada dos años por el Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, requiriendo la aprobación expresa del CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Apoyo Operativo obligará a la automática actualización de éstos, que se llevará a cabo mediante el procedimiento previsto en el apartado primero.

TÍTULO IV

Comunicaciones entre los operadores críticos y las Administraciones públicas

Artículo 33. *Seguridad de las comunicaciones.*

1. El CNPIC será el responsable de administrar los sistemas de gestión de la información y comunicaciones que se diseñen en el ámbito de la protección de las infraestructuras

críticas, que deberá contar para ello con el apoyo y colaboración de los agentes del Sistema y de todos aquellos otros organismos o entidades afectados.

2. La seguridad de los sistemas de información y comunicaciones previstos en este real decreto será acreditada y, en su caso, certificada por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, de acuerdo con las competencias establecidas en su normativa específica.

3. La Presidencia del Gobierno facilitará el uso de la Malla B, sistema soporte de comunicaciones estratégicas seguras del Sistema Nacional de Gestión de Crisis y de la Presidencia del Gobierno, a través del cual los agentes del Sistema autorizados podrán acceder a la información disponible en el Catálogo, con los niveles de acceso que se determinen.

Artículo 34. *El Responsable de Seguridad y Enlace.*

1. En el plazo de tres meses desde su designación como operadores críticos, los mismos nombrarán y comunicarán a la Secretaría de Estado de Seguridad, a través del CNPIC, el nombre del Responsable de seguridad y enlace en los términos y con los requisitos previstos por el artículo 16 de la Ley 8/2011, de 28 de abril.

2. El Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto.

Artículo 35. *El Delegado de Seguridad de la infraestructura crítica.*

1. En el plazo de tres meses desde la identificación como crítica o crítica europea, de una de sus infraestructuras, los operadores críticos comunicarán a las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia e identidad de un Delegado de Seguridad para dicha infraestructura.

2. El Delegado de Seguridad constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica o infraestructura crítica europea de que se trate, encauzando las necesidades operativas e informativas que se refieran a aquélla.

Artículo 36. *Seguridad de los datos clasificados.*

Los datos clasificados relativos a las infraestructuras de los operadores críticos cumplirán, en todo caso, con los requerimientos de seguridad establecidos por el Secretario de Estado Director del Centro Nacional de Inteligencia, de acuerdo con la normativa específica aplicable.

§ 16

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

Ministerio del Interior
«BOE» núm. 224, de 18 de septiembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-10060

El Reglamento de protección de infraestructuras críticas aprobado por el Real Decreto 704/2011, de 20 de mayo, por el que se desarrolla la Ley 8/2011, de 28 de abril, en la que se establecen medidas para la protección de las infraestructuras críticas, dispone en los artículos 22.4 y 25.5 que la Secretaría de Estado de Seguridad establecerá, respectivamente, los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos comprendidos en el artículo 14 de la Ley.

Dichos contenidos mínimos fueron recogidos en la Resolución de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, resolución a su vez modificada por otra, de 29 de noviembre de 2011, que advertía y corregía determinados errores en la primera.

La constante evolución de la amenaza, la implantación de nuevas regulaciones, estrategias y herramientas de planificación, así como la experiencia adquirida en los últimos cuatro años, en buena parte, merced a las aportaciones efectuadas por los propios operadores críticos, hacen aconsejable la actualización de tales contenidos mínimos, con el fin de adecuar el nivel de planificación y respuesta a las exigencias requeridas para una eficaz protección de las infraestructuras críticas nacionales.

En virtud de ello, y conforme a lo preceptuado en el artículo 7, apartado e), del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, resuelvo aprobar y ordenar la publicación en el «Boletín Oficial del Estado» de los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos que se insertan como anexo I y anexo II, respectivamente, de esta resolución.

La presente resolución deroga la precedente en esta misma materia, de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, por la que se establecían los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, así como también la de 29 de noviembre de 2011, que modificaba la anterior.

ANEXO I

Guía Contenidos Mínimos

Plan de Seguridad del Operador (PSO)

Índice

1. Introducción.

1.1 Base legal.

El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada, cuyo funcionamiento es indispensable y no permite soluciones alternativas: las denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población.

Este es precisamente el espíritu de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que tiene como objeto el establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en

materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, impulsando la colaboración e implicación de los organismos y/o empresas gestoras y propietarias (operadores críticos) de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados tanto físicos como lógicos, que puedan afectar a la prestación de los servicios esenciales.

Dicha Ley tiene su desarrollo a través del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El artículo 13 de la Ley explicita una serie de compromisos para los operadores críticos públicos y privados, entre los que se encuentra la necesidad de elaboración de un Plan de Seguridad del operador (en adelante, PSO) y de los Planes de Protección Específicos que se determinen (en adelante, PPE).

Por su parte, el artículo 22.4 del Real Decreto 704/2011 responsabiliza a la Secretaría de Estado de Seguridad (órgano superior responsable del Sistema de Protección de Infraestructuras Críticas Nacionales, conforme al artículo 6 de la Ley 8/2011), a través del CNPIC, del establecimiento y puesta a disposición de los operadores críticos de los contenidos mínimos con los que deben contar los PSO, así como el modelo en el que basar la elaboración de los mismos.

1.2 Objetivo de este Documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe de apoyar un operador crítico a la hora del diseño y elaboración de su PSO. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia.

Igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que estos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los PPE de cada una de sus infraestructuras críticas.

1.3 Finalidad y contenido del PSO.

El PSO definirá la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

El PSO, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá, además de un índice referenciado sobre los contenidos del Plan, información sobre:

- Política general de seguridad del operador y marco de gobierno.
- Relación de Servicios Esenciales prestados por el operador crítico.
- Metodología de análisis de riesgo (amenazas físicas y de ciberseguridad).
- Criterios de aplicación de Medidas de Seguridad Integral.

1.4 Método de revisión y actualización

Conforme al artículo 24 del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador, además de la elaboración y presentación del PSO al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante CNPIC), se incluye su revisión y actualización periódica:

- Revisión: Bienal.
- Actualización: Cuando se produzca algún tipo de modificación en los datos incluidos en el PSO. En este caso, el PSO quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PSO (modificación de datos, identificación de nuevas infraestructuras críticas, baja de infraestructuras críticas, cese de condiciones para ser considerado operador crítico, etc…), el operador deberá trasladar la información oportuna al CNPIC, a través de los

canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la información y documentación.

La información es un valor estratégico para cualquier organización, siendo ésta de carácter sensible, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de esa información, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la ley 08/2011, la clasificación del PSO constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PSO deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el Personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad Física.

OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Política General de Seguridad del Operador y Marco de seguridad.

2.1 Política General de Seguridad del Operador Crítico.

El objetivo de una Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad. En ella, la Dirección de la Organización debe establecer claramente cuáles son sus líneas de actuación y manifestar su apoyo y compromiso con la seguridad.

Por tanto, en este apartado, el operador deberá reflejar el contenido de su Política de Seguridad de una forma homogénea e integral que esté específicamente dirigido al ámbito de las infraestructuras críticas y que sirva de marco de referencia para la protección de las mismas, con el objetivo de impedir su perturbación o destrucción.

Los aspectos mínimos que debe recoger la Política de Seguridad son:

• Objeto: La meta que pretende conseguir la Organización con la política y su posterior desarrollo y aplicación.

• Ámbito o Alcance de Aplicación: Una política puede estar limitada a determinados campos o aspectos o, por el contrario, ser de aplicación a toda la Organización. El operador deberá reflejar sobre qué partes de su Organización es aplicable la Política de Seguridad de protección de infraestructuras críticas, sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la ciberseguridad.

• Compromiso de la Alta Dirección: El operador debe garantizar que a la seguridad debe dársele la misma importancia que a otros factores de la producción o negocio de la organización.

Por ello, el compromiso de la Organización con la Política de Seguridad y lo que de ella se desarrolle deberá quedar plasmado mediante la aprobación, sanción y apoyo de la misma por el órgano (Consejo de Administración, Consejo de Dirección, etc.) o la persona (Presidente, Consejero Delegado, etc.) de gobierno o dirección de la misma con capacidad suficiente para implantarla en la organización, así como su firme y explícito compromiso con la protección de los servicios esenciales prestados, compromiso que se debe ver reflejado en el propio plan.

• Carácter Integral de la Seguridad: La seguridad física y la ciberseguridad son áreas que deben ser abordadas de forma interrelacionada y con una perspectiva holística de la seguridad. Esto redundará en una visión global de la seguridad, posibilitando el diseño de una estrategia corporativa única, y optimizando el conocimiento, los recursos y los equipos. Por ello, el operador deberá remarcar el carácter integral de la seguridad aplicada a sus infraestructuras críticas, indicando en todo caso el procedimiento por el que se pretende alcanzar dicha seguridad integral: aspectos concretos de la organización, estructuras, procedimientos, etcétera. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad física y ciberseguridad.

• Actualización de la Política General de Seguridad del Operador: Al ser la política de seguridad un documento de alto nivel, no suele requerir cambios significativos a lo largo del tiempo. No obstante, el operador deberá asegurarse de que ésta se mantenga actualizada y refleje aquellos cambios requeridos por variaciones en los activos a proteger, del entorno que les pueda afectar (amenazas, vulnerabilidades, impactos, salvaguardas), o en la reglamentación aplicable. En este apartado, el operador deberá recoger el proceso a seguir para la actualización y mantenimiento de su Política de Seguridad, incluyendo la periodicidad y el responsable de llevar a cabo estas acciones.

2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad y Comunicación.

El operador crítico debe designar a un Responsable de Seguridad y Enlace y a los Delegados de Seguridad en cada una de las infraestructuras críticas identificadas, así como a los sustitutos de ambos, de acuerdo a los requisitos establecidos en la Ley 8/2011. Deberá, por tanto, asegurar que se encuentren en un nivel jerárquico suficiente dentro de su estructura organizativa, de tal forma que los designados puedan garantizar el cumplimiento y la aplicación de la Política y de los requisitos establecidos para la protección de las infraestructuras críticas bajo su responsabilidad.

Asimismo, deberá asegurar la presencia física del delegado de seguridad en la infraestructura en un tiempo prudencial, en caso de que ello sea necesario.

En este apartado, el operador crítico deberá describir su organigrama de seguridad (comprendiendo tanto la Seguridad Física como la Ciberseguridad), con indicación de las figuras recogidas en la Ley, así como los niveles jerárquicos que les correspondan en su estructura organizativa.

Dicho organigrama debe incluir la ubicación física, estructura, jerarquía, órgano de gobierno e interrelación de todas las áreas de la organización con responsabilidad en cada uno de los ámbitos de la seguridad corporativa. Además, deberá dejar constancia de que los designados tienen capacidad suficiente para llevar a cabo todas aquellas acciones que se deriven de la aplicación de la Ley y el Real Decreto. En este sentido, el operador crítico deberá presentar:

• Un organigrama general, donde se identifique la estructura de seguridad corporativa.

• Un organigrama específico de la estructura de seguridad que integre la información sobre las distintas funciones que desempeña en la organización.

En su caso, el operador crítico deberá señalar los comités u órganos de decisión existentes en materia de seguridad, así como las funciones de cada uno de ellos.

Igualmente, se reflejarán los procedimientos de gestión y mantenimiento de la seguridad, haciendo constar si éstos son de carácter propio o son subcontratados. En este último caso, será necesario relacionar la empresa o empresas subcontratadas, las certificaciones en materia de seguridad con las que cuentan aquéllas, la sede desde la que se ejercen dichos servicios contratados, así como los servicios y compromisos acordados entre ambos. De igual forma, se definirá la metodología mediante la cual se lleva a cabo la comprobación del cumplimiento por parte de la empresa contratada, con los protocolos de seguridad implementados en su caso por el operador.

En el campo de la ciberseguridad, y en lo relacionado con la protección de infraestructuras críticas, el CERT de Seguridad e Industria (en adelante CERTSI) es el responsable de la resolución de incidencias cibernéticas que puedan afectar a la prestación de los servicios esenciales gestionados por los

El CERTSI, en aplicación del Acuerdo Marco suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas y a la disponibilidad de los servicios que éstos prestan.

Para todo ello, y previa suscripción de un acuerdo de confidencialidad entre las partes (operador crítico – CNPIC – CERTSI), dicho CERT podrá proporcionar servicios de prevención, detección, alerta temprana y respuesta a incidentes en apoyo a los departamentos encargados de esta labor en el seno de cada organización.

2.2.1.1 El Responsable de Seguridad y Enlace.

Conforme al artículo 16.2 de la Ley, el operador crítico deberá nombrar, en el plazo de tres meses desde su designación como tal, al Responsable de Seguridad y Enlace de la organización, que deberá estar habilitado por el Ministerio del Interior como Director de Seguridad, en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, en el que se aprueba el Reglamento de Seguridad Privada, o tener una habilitación equivalente, según su normativa sectorial específica. Tal nombramiento deberá ser comunicado a la Secretaría de Estado de Seguridad, a través del CNPIC.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Responsable de Seguridad y Enlace así como de su sustituto, con idénticas condiciones, en ausencia del titular. Sus funciones en relación con el artículo 34.2 del Real Decreto 704/2011 son las siguientes:

• Representar al operador crítico ante la Secretaria de Estado de Seguridad:

– En materias relativas a la seguridad de sus infraestructuras.
– En lo relativo a los diferentes planes especificados en el Real Decreto.

• Canalizar las necesidades operativas e informativas que surjan entre el operador crítico y el CNPIC.

2.2.1.2 El Delegado de Seguridad de la Infraestructura Crítica.

Conforme al artículo 17 de la Ley, el operador crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la notificación oficial de que es propietario o gestor de al menos una infraestructura crítica o crítica europea.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad, así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación como operador crítico, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

• Ser el enlace operativo y el canal de información con las autoridades competentes en materias relativas a la seguridad de sus infraestructuras.

• Canalizar las necesidades operativas e informativas que surjan, a nivel infraestructura, entre el operador y las autoridades competentes.

2.2.2 Formación y Concienciación.

El operador crítico deberá colaborar con los programas o ejercicios que puedan derivarse del Plan Estratégico Sectorial, así como en su momento de los Planes de Apoyo Operativo.

El operador crítico reflejará en este apartado el Plan de Formación previsto para el personal relacionado con la protección de las infraestructuras críticas, indicando la duración, objetivos que se pretende conseguir, mecanismos de evaluación que se contemplan para el mismo y periodos de actualización. Así mismo, se incluirá el responsable del plan y la capacitación del mismo.

En el caso de que disponga de un Plan de Formación General, especificará la parte relacionada con la protección de las infraestructuras críticas, y la incluirá en este punto.

El operador crítico deberá reflejar en este apartado su participación en ejercicios de simulación en incidentes de seguridad (físicos y cibernéticos), y la periodicidad programada para tales ejercicios.

El personal implicado directamente en la protección de los servicios esenciales e infraestructuras críticas deberá ser formado para alcanzar conocimientos, a nivel básico:

• Sobre seguridad integral (seguridad física y ciberseguridad).
• Sobre autoprotección.
• Sobre seguridad del medio ambiente.
• Sobre habilidades organizativas y de comunicación.
• Sobre sus responsabilidades/actuaciones en caso de materializarse un incidente, o en el caso de que se active un nivel de amenaza 4 ó 5 del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

El personal no directamente implicado deberá ser concienciado mediante la aplicación de las políticas de formación y operacionales activas en la organización.

2.2.3 Modelo de Gestión aplicado.

La seguridad integral depende de un proceso de gestión que debe aportar el control organizativo y técnico necesario para determinar en todo momento el nivel de exposición a las amenazas y el nivel de protección y respuesta que es capaz de proporcionar la organización para la protección y seguridad de sus servicios esenciales e Infraestructuras Críticas.

Por tanto, de acuerdo con la Política de Seguridad marcada, el operador crítico deberá recoger dentro del PSO su modelo de gestión elegido, que deberá contemplar como mínimo:

• Una implementación de controles de seguridad alineada con las prioridades y necesidades evaluadas.

• Una evaluación y monitorización continúa de la seguridad, con identificación de procesos y periodos.

• En el supuesto de que el operador crítico haya diseñado un sistema de gestión y/o la evaluación de la seguridad de las tecnologías de la información, de acuerdo a algún estándar de referencia internacional se debe indicar éste, así como las certificaciones que posee dicho sistema y el organismo certificador.

2.2.4 Comunicación.

El operador crítico deberá recoger explícitamente en este apartado los procedimientos establecidos para la comunicación e intercambio de información relativa a la protección de infraestructuras críticas, de la siguiente manera:

Comunicación al CNPIC:

• De aquellos incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de alguna de las infraestructuras de la que el operador es gestor y/o propietario, conforme al protocolo de comunicación de incidentes PIC elaborado por este Centro y puesto a disposición de los operadores críticos.
• De aquellas variaciones de carácter organizativo, de planificación o estructural que se produzcan en el seno del propio operador y que afecten de alguna manera a las infraestructuras críticas objeto de protección (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

Comunicación al CERTSI:

• A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes del operador crítico y la disponibilidad de los servicios que presta. Todo ello, conforme al protocolo de comunicación de incidentes PIC elaborado por el CNPIC y puesto a disposición de los operadores críticos.

3. Relación de Servicios esenciales prestados por el Operador Crítico.

El PSO deberá incluir, a modo de introducción, la información de contexto suficiente para describir los siguientes aspectos:

• Presentación general del operador crítico y sector/subsector principal/es de su actividad. En caso de grupos empresariales, se identificará claramente, con nombre y CIF, cuál de las empresas es el operador crítico.
• Estructura organizativa y societaria de todo el Grupo (en el caso de grupos empresariales).
• Presencia geográfica en los ámbitos nacional e internacional, con un resumen de las Comunidades Autónomas donde presten sus servicios esenciales, así como de aquellos países donde presten servicios similares.
• Principales líneas de actividad con la tipología general de servicios/productos que ofrecen.

3.1 Identificación de los Servicios esenciales.

El PSO deberá identificar aquellos servicios esenciales para la ciudadanía prestados por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional, en relación al concepto de servicio esencial recogido en el artículo 2. a) de la Ley:

• Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos.
• Eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

3.2 Mantenimiento del inventario de servicios esenciales.

Periódicamente, al menos bienalmente, el operador crítico deberá revisar la relación de servicios esenciales que figuran en su PSO, como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece.
Así, en este mantenimiento deberá incorporar aquellos cambio/s que se produzcan:

• Por causas endógenas (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).
• Como consecuencia de la adecuación a los períodos establecidos en el Plan conforme al punto 1.4 de esta guía.

3.3 Estudio de las consecuencias de la interrupción del servicio esencial.

El operador crítico deberá llevar a cabo un estudio de las consecuencias que supondría la interrupción y no disponibilidad del servicio esencial que presta a la sociedad, motivado por:

• Alteración o interrupción temporal del servicio prestado.
• Destrucción parcial o total de la infraestructura que gestiona el servicio.

Adicionalmente, deberá identificar claramente, para cada uno de los casos anteriores, la siguiente información:

• Extensión geográfica y número de personas que pueden verse afectadas.
• Efecto sobre operadores y servicios esenciales dependientes.
• Existencia de alternativas de prestación del servicio esencial o mecanismos de contingencia proporcionados por el propio operador y nivel de degradación que conllevan.

3.4 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en otros sectores diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores en el marco global de su organización.

El operador crítico deberá hacer referencia a las interdependencias que identifique, explicando en líneas generales el motivo que origina dichas dependencias:

• Entre sus propias instalaciones o servicios.
• Con operadores del mismo sector.
• Con operadores de distintos sectores.
• Con operadores de otros países, del mismo sector o no.
• Con sus proveedores de servicio dentro de la cadena de suministros.
• Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.

4. Metodología del Análisis de Riesgos.

En virtud de lo establecido en el artículo 22.3 del Real Decreto 704/2011, en el PSO se plasmará la metodología o metodologías de análisis de riesgos empleadas por el operador crítico. Dichas metodologías deberán estar internacionalmente reconocidas, garantizar la continuidad de los servicios proporcionados por dicho operador y contemplar, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos críticos. Todo ello, con independencia de las medidas mínimas que se puedan establecer para los Planes de Protección Específicos conforme a lo establecido por el artículo 25.

4.1 Descripción de la metodología de análisis.

Se describirá de forma genérica la metodología empleada por la Organización para la realización de los análisis de riesgos de los diferentes Planes de Protección Específicos (PPE) que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

• Etapas esenciales.
• Algoritmos de cálculo empleados.
• Método empleado para la valoración de los impactos.
• Métricas de medición de riesgos aceptables, residuales, etc.
• En particular, se harán constar las relaciones entre los análisis de riesgos realizados a distintos niveles: A nivel de corporación, a nivel de servicios y el más concreto, a nivel de infraestructuras críticas.

4.2 Tipologías de activos que soportan los servicios esenciales.

Se denominan activos los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Sobre la base de los servicios identificados en el apartado 3.1 anterior, se incluirán en este apartado, para cada servicio esencial, los tipos de activos que los soportan, diferenciando aquéllos que son críticos de los que no lo son.

Las tipologías de activos a considerar serán, al menos:

• Las instalaciones necesarias para la prestación del servicio esencial.
• Los sistemas informáticos necesarios para dar soporte a los servicios esenciales (hardware y software).
• Las redes de comunicaciones necesarias para la prestación del servicio esencial.
• Las personas que explotan u operan todos los elementos anteriormente citados.

El objeto de esta sección es la identificación genérica de tipologías de activos asociadas a los servicios esenciales prestados por dicho operador, y sobre los que se focalizará el análisis de riesgos que efectúe el operador. El nivel de detalle será aquel que permita una comprensión del funcionamiento de los servicios, así como las interrelaciones entre activos y servicios.

Los activos no serán necesariamente espacios físicos concretos, pudiendo por ejemplo considerarse como activos sistemas distribuidos, tales como una red de datos.

4.3 Identificación y evaluación de amenazas.

En el marco de la normativa de protección de infraestructuras críticas y de cara a garantizar la adecuada protección de aquellas infraestructuras que prestan servicios esenciales, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

• Las intencionadas, de tipo tanto físico como lógico, que puedan afectar al conjunto de sus infraestructuras, las cuales deberán identificarse de forma específica en sus respectivos PPE, en su caso.
• Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.

4.4 Valoración y Gestión de Riesgos.

Los PSO recogerán la estrategia de gestión de riesgos implementada por el operador en cuanto a:

• Criterios utilizados para la valoración de las categorías de clasificación de los riesgos.
• Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.).
• Plazos para la implantación de medidas, en el caso de elegir una estrategia de minimización del riesgo con indicación, si existe, de mecanismos de priorización de acciones.
• Tratamiento dado a las amenazas de ataques deliberados y, en particular, a aquellas que tengan una baja probabilidad pero un alto impacto debido a las consecuencias por su destrucción o interrupción en la continuidad de los servicios esenciales.
• Mecanismos de seguimiento y actualización periódicos de niveles de riesgo.

5. Criterios de aplicación de medidas de seguridad integral.

Dentro del ámbito de la seguridad integral, el operador definirá a grandes rasgos los criterios utilizados en su organización para la aplicación y administración de la seguridad. En este sentido, incluirá de forma genérica las medidas de seguridad implantadas en el conjunto de activos y recursos sobre los que se apoyan los servicios esenciales y que se recogerán en sus respectivos PPE, al objeto de hacer frente a las amenazas físicas y lógicas identificadas en los oportunos análisis de riesgos efectuados sobre cada una de las tipologías de sus activos.

6. Documentación complementaria.

6.1 Normativa, buenas prácticas y regulatoria.

El operador recogerá en una breve referencia motivada toda la normativa de aplicación y aquellas buenas prácticas que regulen el buen funcionamiento de los servicios esenciales prestados por todas y cada una de sus infraestructuras.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

- Seguridad Física.
- Ciberseguridad.
- Seguridad de la Información.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

6.2 Coordinación con otros Planes.

Se identificarán todos aquellos Planes diseñados por el operador relativos a otros aspectos (continuidad de negocio, gestión del riesgo, respuesta, ciberseguridad, autoprotección, emergencias, etc.) que puedan coordinarse con el Plan de Seguridad del operador y los respectivos Planes de Protección Específicos que serán activados en el caso de que las medidas preventivas fallen y se produzca un incidente. Así mismo, debe dejarse constancia de la coordinación existente con el Plan Nacional para la Protección de las Infraestructuras Críticas.

ANEXO II

Guía de contenidos mínimos

Plan de Protección Específico (PPE)

Índice

1. Introducción.

1.1 Base Legal.
1.2 Objetivo de este Documento.
1.3 Finalidad y Contenido del PPE.
1.4 Método de Revisión y Actualización.
1.5 Protección y Gestión de la Información y Documentación.

2. Aspectos Organizativos.

2.1 Organigrama de Seguridad.
2.2 Delegados de Seguridad de las Infraestructuras Críticas.
2.3 Mecanismos de Coordinación.
2.4 Mecanismos y Responsables de Aprobación.

3. Descripción de la Infraestructura Crítica.

3.1 Datos Generales de la infraestructura crítica.
3.2 Activos/Elementos de la infraestructura crítica.
3.3 Interdependencias.

4. Resultados del Análisis de Riesgos.

4.1 Amenazas Consideradas.
4.2 Medidas de Seguridad Integral existentes.

4.2.1 Organizativas o de Gestión.
4.2.2 Operacionales o Procedimentales.
4.2.3 De Protección o Técnicas.

4.3 Valoración de Riesgos.

5. Plan de Acción propuesto (por activo).

6. Documentación complementaria.

1. Introducción.

1.1 Base legal.

Según establece la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico, ya sea éste perteneciente al sector público o al privado, se integrará como agente del sistema de protección de infraestructuras críticas, debiendo cumplir con una serie de responsabilidades recogidas en su artículo 13.

De acuerdo con en el punto 1, letra «d», del citado artículo, el operador deberá elaborar un Plan de Protección Específico (en adelante, PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, a través del cual se da desarrollo reglamentario a la Ley 8/2011, establece, en su capítulo IV del Título III sobre los Instrumentos de Planificación, aquellos aspectos relativos a la elaboración, finalidad y contenido de dichos planes, además de su aprobación o modificación, registro, clasificación y formas de revisión y actualización, así como las autoridades encargadas de su aplicación y seguimiento, y la compatibilidad con otros planes ya existentes.

En este sentido, y conforme al artículo 25.5 de dicho real decreto, se asigna a la Secretaría de Estado de Seguridad, a través del Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC), la responsabilidad de establecer los contenidos mínimos de los PPE, así como el modelo en el que fundamentar su estructura y compleción, sobre la base de las directrices y criterios marcados por el Plan de Seguridad del Operador (en adelante, PSO).

En el PPE, el operador crítico aplicará los siguientes aspectos y criterios incluidos en su PSO, que afecten de manera específica a esa instalación:

• Aspectos relativos a su política general de seguridad.
• Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica.
• Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como aquellas que afectan a la ciberseguridad, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

1.2 Objetivo de este documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe apoyar el operador crítico a la hora de elaborar su respectivo PPE en las instalaciones catalogadas como críticas. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la Ley 8/2011 y el Real Decreto 704/2011.

1.3 Finalidad y contenido del PPE.

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y ciberseguridad) de sus infraestructuras críticas.

Además de un índice referenciado a los contenidos del Plan, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

• Organización de la seguridad.
• Descripción de la infraestructura.
• Resultado del análisis de riesgos:

Medidas de seguridad integral (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional de acuerdo con lo establecido por el Plan de Prevención y Protección Antiterrorista y por el Plan Nacional de Protección de Infraestructuras Críticas.

• Plan de acción propuesto (por cada activo evaluado en el análisis de riesgos).

Los PPE deberán estar alineados con las pautas establecidas en la Política General de Seguridad del operador reflejada en el PSO. Así mismo, los análisis de riesgos, vulnerabilidades y amenazas que se lleven a cabo, estarán sujetos a las pautas metodológicas descritas en el PSO.

1.4 Método de Revisión y Actualización.

Conforme al artículo 27 del Real Decreto por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador crítico, además de la elaboración y presentación del PPE al CNPIC, se incluye su revisión y actualización periódica:

• Revisión: Bienal, que deberá ser aprobada por las Delegaciones del Gobierno en las CC.AA. y las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, además de por parte del CNPIC.

• Actualización: Cuando se produzca una modificación en los datos incluidos dentro del PPE. En este caso, el PPE quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PPE (organización de la seguridad, datos de descripción de la infraestructura, medidas de seguridad, etc…), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la Información y Documentación.

La información asociada con los PPE y aquélla relativa a los análisis de riesgos y las medidas de seguridad implantadas sobre las infraestructuras críticas a las que hacen referencia es de carácter sensible, por lo que, en este sentido, el operador deberá definir sus procedimientos de tratamiento de dicha información, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de la información utilizados, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la Ley 08/2011, la clasificación del PPE constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PPE deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04.–Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad física.

OR-ASIP-01-01.03.–Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03.–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04.–Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Aspectos organizativos.

2.1 Organigrama de seguridad.

El operador crítico debe presentar gráficamente la estructura organizativa funcional que en materia de seguridad integral existe en la infraestructura crítica, con indicación de todos los actores que participan en aquella, su rol de responsabilidad y su jerarquía en el proceso de toma de decisiones. Del mismo modo, se debe establecer la dependencia de esta estructura con aquella definida en el correspondiente Plan de Seguridad del Operador.

2.2 Delegados de Seguridad de las Infraestructuras Críticas.

Conforme al artículo 17 de la Ley 8/2011, el operador crítico con infraestructuras designadas como críticas o criticas europeas comunicará a las Delegaciones del Gobierno en las CC.AA. y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquellas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la designación de una infraestructura como crítica.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

• Ser el enlace operativo y el canal de información con las autoridades competentes en materia relativa a la seguridad de sus infraestructuras.

• Canalizar las necesidades operativas e informativas que surjan.

El operador crítico deberá reflejar en este apartado los cursos o formación que el Delegado de Seguridad haya recibido, relacionados con las habilidades necesarias para el desempeño del puesto, de acuerdo con el Plan de Formación previsto en el PSO.

2.3 Mecanismos de Coordinación.

El operador crítico deberá reflejar dentro de su PPE los mecanismos existentes de coordinación:

• Entre el Delegado de Seguridad de la infraestructura crítica con otros Delegados de otras infraestructuras críticas y con el Responsable de Seguridad y Enlace del propio operador.

• Con autoridades y terceros (Fuerzas y Cuerpos de Seguridad del Estado/Cuerpos Policiales autonómicos y locales/CNPIC/otros).

• Con otros planes existentes del operador (planes de continuidad de negocio, planes de evacuación, etc.).

• Con el CERT de Seguridad e Industria (CERTSI) identificando los puntos de contacto del operador en los 3 niveles requeridos: el institucional, y el directivo y el técnico, todos ellos referidos a en la gestión de incidentes.

• Con los proveedores críticos que se especifiquen a tenor del desarrollo de lo establecido en el punto 3.2.

2.4 Mecanismos y responsables de aprobación.

El operador deberá incluir dentro del PPE los siguientes aspectos relativos a su aprobación y revisión interna:

• Responsables de su aprobación.
• Procedimiento que se sigue para su aprobación.
• Fecha en la que se produjo su última aprobación.
• Responsable de su revisión y actualización.
• Aspectos objeto de revisión, en su caso.
• Registros generados por el procedimiento de revisión que permitan comprobar que el PPE ha sido revisado (reuniones, acta del Comité correspondiente, estudios y análisis realizados, actualizaciones de los análisis de riesgos, etc.).

3. Descripción de la Infraestructura Crítica.

3.1 Datos generales de la infraestructura crítica.

El operador crítico deberá incluir los siguientes datos e información sobre la infraestructura a proteger:

• Generales, relativos a la denominación y tipo de instalación, propiedad y gestión de la misma.
• Sobre localización física y estructura (localización, planos generales, fotografías, componentes, etc.)
• Sobre los sistemas TIC que gestionan la infraestructura crítica y su arquitectura.
• Datos estratégicos:

Descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional del mismo.
Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.
Descripción de sus funciones y de su relación con los servicios esenciales soportados.

3.2 Activos/elementos de la infraestructura críticas.

Se incluirán en este apartado todos los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

• Las instalaciones o componentes de la infraestructura crítica que son necesarios y por lo tanto vitales para la prestación del servicio esencial.
• Los sistemas informáticos (hardware y software) utilizados, con especificación de los fabricantes, modelos y, versiones, etcétera.
• Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha infraestructura crítica:

Arquitectura de red, rangos de IP públicas y, dominios.
Esquema(s) de red completo y detallado, de tipo gráfico y con descripción literaria, donde se recojan los flujos de intercambio de información que se realizan en las redes, así como sus perímetros electrónicos.
Descripción de componentes de la red (servidores, terminales, hubs, switches, nodos, routers, firewalls,…) así como su ubicación física.

• Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados, indicando y detallando de forma particular si existe algún proceso externalizado a terceros.
• Los proveedores críticos que en general son necesarios para el funcionamiento de dicha infraestructura crítica, y específicamente:

De suministro eléctrico.
De comunicaciones (telefonía, internet, etc. …).
De tratamiento y almacenamiento de información (CPDs, etc.).
De ciberseguridad (CERTs privados, SOCs, etc.).

• Sobre los proveedores nombrados por el operador, se especificarán los distintos Acuerdos de Nivel de Servicios que se tienen contratados y que son considerados esenciales.

Del mismo modo, se especificarán las interdependencias existentes entre los diferentes activos que soportan o componen la infraestructura crítica. La información anterior deberá ser la suficiente para recoger de manera explícita el alcance de la infraestructura a proteger y con el mismo nivel de detalle que se haya establecido dentro del PSO.

3.3 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores para la infraestructura crítica de que se trate, en el marco del PPE.

El operador crítico deberá hacer referencia dentro de sus diferentes PPE a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

• Con otras infraestructuras críticas del propio operador.
• Con otras infraestructuras estratégicas del propio operador que soportan el servicio esencial.
• Entre sus propias instalaciones o servicios.
• Con sus proveedores dentro de la cadena de suministro.
• Con los proveedores de servicios TIC contratados para esa infraestructura, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.
• Con los proveedores de servicios de seguridad física, indicando los servicios prestados y el personal y medios empleados.

4. Resultados del Análisis de Riesgos.

El operador crítico deberá reflejar en su PPE los resultados del análisis de riesgos integral realizado sobre la infraestructura crítica. Dicho análisis de riesgos deberá seguir las pautas metodológicas recogidas en su PSO.

A continuación se reflejan los contenidos mínimos relativos al análisis de riesgos realizado que el operador deberá incluir dentro del PPE.

4.1 Amenazas consideradas.

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de las infraestructuras críticas, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

• Las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica.
• Las amenazas que puedan afectar directamente a la infraestructura procedente de las interdependencias identificadas, sean éstas deliberadas o no.
• Las dirigidas al entorno cercano o elementos interdependientes tanto del ante-perímetro físico como lógico que puedan afectar a la infraestructura.
• Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.

• Las amenazas que afecten a los sistemas y servicios que soportan la seguridad integral.

4.2 Medidas de seguridad integral existentes.

El operador deberá describir las medidas de seguridad integral (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación) implantadas en la actualidad, con las que se ha contado para la realización del análisis de riesgos. Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales.

Por medidas permanentes se entienden aquellas medidas concretas ya adoptadas por el operador crítico, así como aquellas que considere necesarias instalar en función del resultado del análisis de riesgo realizado respecto de los riesgos, amenazas y consecuencias/impacto sobre sus activos, dirigidas todas ellas a garantizar la seguridad integral de su instalación catalogada como crítica de manera continua.

Por medidas temporales y graduales se entienden aquellas medidas de seguridad de carácter extraordinario que reforzarán a las permanentes y que se deberán implementar de forma ascendente a raíz de la activación de alguno de los niveles de seguridad establecidos respectivamente en el Plan Nacional de Protección de las Infraestructuras Críticas (artículo 16.3 del RD 704/2011), en coordinación con el Plan de Prevención y Protección Antiterrorista, principalmente para los niveles 4 y 5, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta y temporal sobre la instalación por él gestionada.

Dichas medidas deberán permanecer activas durante el tiempo que esté establecido el nivel de alarma, modificándose gradualmente en función de dicho nivel.

Para su mejor comprensión, se recomienda una aproximación por capas para cada nivel, siendo la escala de niveles del 1 al 5 (nivel 1: riesgo bajo; nivel 2: riesgo moderado; nivel 3 riesgo medio; nivel 4: riesgo alto; nivel 5: riesgo muy alto), especificando para cada nivel las medidas de prevención y protección, el tiempo de respuesta y el tiempo de recuperación.

En concreto, el operador deberá describir las medidas concretas de que dispone relativas a:

4.2.1 Organizativas o de Gestión.

El operador deberá indicar si dispone de al menos de las siguientes medidas organizativas o de gestión, y el alcance de cada una de ellas:

• Análisis de Riesgos: Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo.
• Definición de roles y responsabilidades: Asignación de responsabilidades en materia de seguridad.
• Cuerpo normativo definido: Políticas, procedimientos y estándares de seguridad.
• Normas y/o regulaciones de aplicación a la infraestructura crítica, así como identificación de su nivel de cumplimiento.
• Certificación, acreditación y evaluación de seguridad obtenidas para la infraestructura crítica.

4.2.2 Operacionales o Procedimentales.

El operador deberá indicar si dispone de al menos las siguientes medidas operacionales o procedimentales, y el alcance de cada una de ellas.

• Procedimientos para la realización, gestión y mantenimiento de activos críticos (ciclo de vida):

Identificación.
Adquisición.
Catalogación.
Alta.
Actualización.
Baja.

• Procedimientos de formación, concienciación y capacitación (tanto general como específica) para:

Empleados/Operarios.
Personal de seguridad.
Personal contratado.
Etc.

• Procedimientos de Contingencia/Recuperación, en función de los escenarios de contingencia que hayan sido definidos. Se deben detallar además los métodos y políticas de copias de respaldo (backup).
• Procedimientos operativos para la monitorización, supervisión y evaluación/auditoría de:

Activos Físicos de la infraestructura (Alcance/Operación/Seguimiento).
Activos Lógicos o de sistemas de operación (Alcance/Operación/Seguimiento).

• Procedimientos de seguridad.
• Procedimientos para la gestión de acceso:

Gestión de usuarios: Altas, bajas y modificaciones, procesos de selección, régimen interno, procedimientos de cese.
Control de accesos temporales:

De personas, vehículos, etc. al recinto general o a recintos restringidos.
Identificadores de usuario temporal de los sistemas (mantenimiento…).

Control de entradas y salidas:

Paquetería, correspondencia, etc.
Soportes, equipos e información (medidas y tecnologías de prevención de fuga de información).

• Procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).
• Procedimientos de gestión y respuesta ante amenazas e incidentes.
• Procedimientos de comunicación e intercambio de información relativos a la protección de infraestructuras críticas (a través del protocolo de incidentes proporcionado por el CNPIC al efecto):

Con el CNPIC:

Sobre incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de la infraestructura.
Sobre variación de datos sobre la organización y medidas de seguridad, datos de descripción de la infraestructura, etc.

Con el CERTSI:

A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes de la infraestructura y la disponibilidad de los servicios por ella prestada.

4.2.3 De Protección o Técnicas.

• Medidas de Prevención y Detección:

Medidas y elementos de seguridad física y electrónica para la protección del perímetro y control de accesos:

Vallas, zonas de seguridad, detectores de intrusos, cámaras de video vigilancia/CCTV, puertas y esclusas, cerraduras, lectores de matrículas, arcos de seguridad, tornos, scanners, tarjetas activas, lectores de tarjetas, etc.

Medidas y elementos de ciberseguridad:

• Firewalls, DMZ, IPSs, IDSs, segmentación y aislamiento de redes, cifrado, VPNs, elementos y medidas de control de acceso de usuarios (tokens, controles biométricos, etc.), medidas de instalación y configuración segura de elementos técnicos, correladores de eventos y logs, protección frente Malware, etc.

Redundancia de sistemas (hardware y software).

Otros.

• Medidas de Coordinación y Monitorización:

Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.).

Equipos de vigilancia (turnos, rondas, volumen, etc.).

Sistemas de comunicación.

Otros.

4.3 Valoración de riesgos.

En este apartado se describirán las principales conclusiones obtenidas en el análisis de riesgos. Para cada par activo/amenaza se deberá especificar la valoración efectuada, sobre la base de los criterios especificados en la metodología de análisis de riesgos detallada en el PSO. Dentro de este apartado deberá incluirse, para cada par activo/amenaza, la siguiente información:

• Quién ha evaluado/aprobado el riesgo y la estrategia de tratamiento asociada.
• Criterios de valoración de riesgos adoptados.
• Fecha del último análisis llevado a cabo.
• Resultado/conclusión sobre el nivel de riesgo soportado.
• Evolución en el tiempo de la evaluación del par activo/amenaza

En particular, deberán detallarse los riesgos asumidos en activos con niveles de impacto elevado y baja probabilidad de ocurrencia, que deberán ser validados por el CNPIC.

5. Plan de acción propuesto (por activo).

En caso de ser pertinente y preverse la disposición de medidas complementarias a las existentes a implementar en los próximos tres años, se deberá describir, como parte integrante del PPE:

• Listado de las medidas complementarias a disponer (físicas o de ciberseguridad).
• Una explicación de la operativa resultante para cada tipo de protección (físico y lógico).

El operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos. En concreto, deberá incluir la siguiente información:

• Activo de aplicación.
• Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
• Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
• Carácter de la medida, permanente, temporal o gradual.

6. Documentación complementaria.

El operador crítico incorporará como anexo la planimetría general de la instalación o sistema y de sus sistemas de información, así como aquellos otros planos que incorporen la ubicación de las medidas de seguridad implementadas. A su vez, se podrá adjuntar aquella otra información que se pueda generar de los diferentes apartados de este documento.

Se hará una breve referencia a todos aquellos planes de diferente tipo (emergencia, autoprotección, ciberseguridad, etc.), que afecten a la instalación o sistema con el fin de establecer una adecuada coordinación entre ellos, así como toda aquella normativa y buenas prácticas que regulen el buen funcionamiento del servicio esencial prestado por esa infraestructura y los motivos por los cuales le son de aplicación.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

- Seguridad Física.
- Ciberseguridad.
- Seguridad de la Información.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

§ 17

Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía. [Inclusión parcial]

Ministerio del Interior
«BOE» núm. 21, de 24 de enero de 2013
Última modificación: 15 de julio de 2016
Referencia: BOE-A-2013-662

[. . .]

CAPÍTULO I

Organización central

[. . .]

Artículo 7. *Comisaría General de Policía Judicial.*

Estará integrada por las siguientes unidades:

1. Secretaría General.

En su función de apoyo y asistencia a la Comisaría General, analiza y planifica sus líneas generales de actuación, y gestiona los asuntos relativos al régimen de personal y medios adscritos a la misma. Se responsabiliza de las bases de datos propias de la Comisaría General. Elabora las metodologías de investigación criminal y lleva a cabo estudios técnicos y jurídicos para el perfeccionamiento de las actividades operativas.

El Secretario General, como segundo jefe de la Comisaría General, sustituye a su titular, en los casos de vacante, ausencia o enfermedad.

2. Unidad Central de Droga y Crimen Organizado.

Asume la investigación y persecución de las actividades delictivas, de ámbitos nacional y transnacional, relacionadas con el tráfico de drogas, con arreglo a las competencias atribuidas en el artículo 12. 1 A) e) de la LO 2/1986, de 13 de marzo, y el crimen organizado, así como la coordinación operativa y el apoyo técnico de las respectivas unidades territoriales. De esta Unidad dependerán:

a) La Brigada Central de Estupefacientes, que asume las competencias de investigación y persecución de los delitos relacionados con el tráfico ilegal de drogas, con arreglo a la legislación sobre la materia.

b) La Brigada Central de Crimen Organizado, que asume la investigación y persecución de las actividades delictivas vinculadas a la delincuencia organizada y la dirección de los Grupos de Respuesta contra el Crimen Organizado desplegados en diversas zonas del territorio español.

c) La Unidad Adscrita a la Fiscalía General del Estado, que desempeñará los cometidos que, como Policía Judicial, le asigne el órgano al que figura adscrita.

3. Unidad Central de Delincuencia Especializada y Violenta.

Asume la investigación y persecución de las actividades delictivas, de ámbito nacional y transnacional, en lo concerniente a delitos contra las personas; a delitos relacionados con el patrimonio, especialmente el patrimonio histórico artístico; las relativas al derecho de autor; al consumo y medio ambiente; a las infracciones delictivas en materia de dopaje en el deporte; a la vigilancia e inspección del juego; así como la coordinación operativa y el apoyo técnico de las respectivas unidades territoriales.

De esta Unidad dependerán:

a) La Brigada Central de Investigación de la Delincuencia Especializada, encargada de la investigación y persecución de los delitos relacionados con el patrimonio, el consumo y el medio ambiente, propiedad intelectual e industrial. De esta Brigada dependerá el Servicio de Control de Juegos de Azar, con la misión de vigilancia e inspección del cumplimiento de la normativa sobre el juego e investigación de los delitos que se generen en este ámbito.

b) La Brigada Central de Investigación de Delitos contra las Personas, encargada de la investigación y persecución de los delitos contra la vida, la libertad, homicidios y desaparecidos.

c) La Brigada del Patrimonio Histórico, encargada de la investigación y persecución de las actividades delictivas relacionadas con el patrimonio histórico artístico.

4. Unidad Central de Inteligencia Criminal.

Da apoyo al titular de la Comisaría General en sus funciones de dirección, planificación y toma de decisiones. En el marco de su ámbito competencial y, como parte de la estructura nacional de inteligencia y planificación, se responsabiliza de la captación, recepción, análisis, tratamiento y desarrollo de las informaciones relativas a la criminalidad, así como la elaboración, desarrollo y seguimiento y control de planes estratégicos y operativos, y la actividad prospectiva.

5. Unidad Central de Delincuencia Económica y Fiscal.

Asume la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y el apoyo técnico a las respectivas Unidades territoriales. De esta Unidad dependerán:

a) La Brigada Central de Delincuencia Económica y Fiscal, a la que le corresponde la investigación de los delitos relacionados contra las Haciendas Públicas, contra la Seguridad Social, sus Entidades Gestoras en sus distintas modalidades, y los delitos contra los derechos de los trabajadores, fraudes financieros, fraudes en los medios de pago, delitos bursátiles, espionaje industrial y estafas de especial trascendencia.

b) La Brigada Central de Investigación de Blanqueo de Capitales y Anticorrupción, a la que corresponde la investigación de hechos delictivos relacionados con el blanqueo de capitales procedente de hechos delictivos, los delitos económicos relacionados con la piratería internacional, la corrupción en sus distintas modalidades y la localización y la recuperación de activos.

c) La Brigada Central de Inteligencia Financiera, a la que corresponde la investigación y persecución de los hechos delictivos relacionados con las actividades y sujetos regulados por la normativa de prevención del blanqueo de capitales.

d) La Brigada de Investigación del Banco de España, que asume la investigación y persecución de los delitos relacionados con la falsificación de moneda nacional y extranjera, funcionando como Oficina Central Nacional a este respecto.

e) La Unidad Adscrita a la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada, que desempeñará los cometidos que, como Policía Judicial, le asigne el órgano al que figura adscrita.

6. Unidad de Investigación Tecnológica.

Asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía.

De esta Unidad dependerán:

a) La Brigada Central de Investigación Tecnológica, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones.

b) La Brigada Central de Seguridad Informática la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes.

7. Unidad Central de Atención a la Familia y Mujer.

Asume la investigación y persecución de las infracciones penales en el ámbito de la violencia de género, doméstica y todos los delitos sexuales con independencia de la relación entre víctima y autor, al igual que la coordinación de la actividad de protección de las víctimas de violencia de género.

De esta Unidad dependerán:

a) La Brigada Operativa Atención a la Familia y Mujer, a la que le corresponde la coordinación de la actuación de la función de investigación y persecución de los delitos cometidos en el ámbito familiar y contra la mujer, así como la de protección de las víctimas en materia de violencia de género.

b) El Gabinete de Estudios, al que corresponde el seguimiento y análisis en el ámbito policial de todos los delitos conocidos, promoviendo iniciativas y medidas dirigidas a la lucha contra el problema social que estas violencias suponen; y la coordinación con otros organismos nacionales e internacionales con competencia en estas materias.

Se constituye, dentro del Cuerpo Nacional de Policía, como único punto de contacto y referencia en esta materia.

[. . .]

§ 18

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana

Jefatura del Estado
«BOE» núm. 77, de 31 de marzo de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-3442

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

I

La seguridad ciudadana es la garantía de que los derechos y libertades reconocidos y amparados por las constituciones democráticas puedan ser ejercidos libremente por la ciudadanía y no meras declaraciones formales carentes de eficacia jurídica. En este sentido, la seguridad ciudadana se configura como uno de los elementos esenciales del Estado de Derecho.

Las demandas sociales de seguridad ciudadana van dirigidas esencialmente al Estado, pues es apreciable una conciencia social de que sólo éste puede asegurar un ámbito de convivencia en el que sea posible el ejercicio de los derechos y libertades, mediante la eliminación de la violencia y la remoción de los obstáculos que se opongan a la plenitud de aquellos.

La Constitución Española de 1978 asumió el concepto de seguridad ciudadana (artículo 104.1), así como el de seguridad pública (artículo 149.1.29.ª). Posteriormente, la doctrina y la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana.

Es a la luz de estas consideraciones como se deben interpretar la idea de seguridad ciudadana y los conceptos afines a la misma, huyendo de definiciones genéricas que justifiquen una intervención expansiva sobre los ciudadanos en virtud de peligros indefinidos, y evitando una discrecionalidad administrativa y una potestad sancionadora genéricas.

Para garantizar la seguridad ciudadana, que es una de las prioridades de la acción de los poderes públicos, el modelo de Estado de Derecho instaurado por la Constitución

dispone de tres mecanismos: un ordenamiento jurídico adecuado para dar respuesta a los diversos fenómenos ilícitos, un Poder Judicial que asegure su aplicación, y unas Fuerzas y Cuerpos de Seguridad eficaces en la prevención y persecución de las infracciones.

En el marco del artículo 149.1.29.ª de la Constitución y siguiendo las orientaciones de la doctrina constitucional, esta Ley tiene por objeto la protección de personas y bienes y el mantenimiento de la tranquilidad ciudadana, e incluye un conjunto plural y diversificado de actuaciones, de distinta naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico protegido. Una parte significativa de su contenido se refiere a la regulación de las intervenciones de la policía de seguridad, funciones propias de las Fuerzas y Cuerpos de Seguridad, aunque con ello no se agota el ámbito material de lo que hay que entender por seguridad pública, en el que se incluyen otras materias, entre las que la Ley aborda las obligaciones de registro documental o de adopción de medidas de seguridad por las personas físicas o jurídicas que realicen actividades relevantes para la seguridad ciudadana, o el control administrativo sobre armas y explosivos, entre otras.

II

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, constituyó el primer esfuerzo por abordar, desde la óptica de los derechos y valores constitucionales, un código que recogiera las principales actuaciones y potestades de los poderes públicos, especialmente de las Fuerzas y Cuerpos de Seguridad, a fin de garantizar la seguridad de los ciudadanos.

Sin embargo, varios factores aconsejan acometer su sustitución por un nuevo texto. La perspectiva que el transcurso del tiempo ofrece de las virtudes y carencias de las normas jurídicas, los cambios sociales operados en nuestro país, las nuevas formas de poner en riesgo la seguridad y la tranquilidad ciudadanas, los nuevos contenidos que las demandas sociales incluyen en este concepto, la imperiosa necesidad de actualización del régimen sancionador o la conveniencia de incorporar la jurisprudencia constitucional en esta materia justifican sobradamente un cambio legislativo.

Libertad y seguridad constituyen un binomio clave para el buen funcionamiento de una sociedad democrática avanzada, siendo la seguridad un instrumento al servicio de la garantía de derechos y libertados y no un fin en sí mismo.

Por tanto cualquier incidencia o limitación en el ejercicio de las libertades ciudadanas por razones de seguridad debe ampararse en el principio de legalidad y en el de proporcionalidad en una triple dimensión: un juicio de idoneidad de la limitación (para la consecución del objetivo propuesto), un juicio de necesidad de la misma (entendido como inexistencia de otra medida menos intensa para la consecución del mismo fin) y un juicio de proporcionalidad en sentido estricto de dicha limitación (por derivarse de ella un beneficio para el interés público que justifica un cierto sacrificio del ejercicio del derecho).

Son estas consideraciones las que han inspirado la redacción de esta Ley, en un intento de hacer compatibles los derechos y libertades de los ciudadanos con la injerencia estrictamente indispensable en los mismos para garantizar su seguridad, sin la cual su disfrute no sería ni real ni efectivo.

III

La Ley, de acuerdo con la jurisprudencia constitucional, parte de un concepto material de seguridad ciudadana entendida como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad de los ciudadanos, que engloba un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico así definido. Dentro de este conjunto de actuaciones se sitúan las específicas de las organizaciones instrumentales destinadas a este fin, en especial, las que corresponden a las Fuerzas y Cuerpos de Seguridad, a las que el artículo 104 de la Constitución encomienda proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Junto a esas actividades policiales en sentido estricto, la Ley regula aspectos y funciones atribuidos a otros órganos y autoridades administrativas, como la documentación e identificación de las personas, el control administrativo de armas, explosivos, cartuchería y artículos pirotécnicos o la previsión de la necesidad de adoptar

medidas de seguridad en determinados establecimientos, con el correlato de un régimen sancionador actualizado imprescindible para garantizar el cumplimiento de los fines de la Ley.

La Ley se estructura en cinco capítulos divididos en cincuenta y cuatro artículos, siete disposiciones adicionales, una transitoria, una derogatoria y cinco finales.

El capítulo I, tras definir el objeto de la Ley, recoge como novedades más relevantes sus fines y los principios rectores de la actuación de los poderes públicos en el ámbito de la seguridad ciudadana, la cooperación interadministrativa y el deber de colaboración de las autoridades y los empleados públicos, los distintos cuerpos policiales, los ciudadanos y las empresas y el personal de seguridad privada, de acuerdo con una perspectiva integral de la seguridad pública. Entre los fines de la Ley destacan la protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico; la garantía del normal funcionamiento de las instituciones; la preservación no sólo de la seguridad, sino también de la tranquilidad y la pacífica convivencia ciudadanas; el respeto a las Leyes en el ejercicio de los derechos y libertades; la protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección; la pacífica utilización de vías y demás bienes demaniales destinados al uso y disfrute público; la garantía de la normal prestación de los servicios básicos para la comunidad; y la transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana.

El capítulo II regula la documentación e identificación de los ciudadanos españoles, el valor probatorio del Documento Nacional de Identidad y del pasaporte y los deberes de los titulares de estos documentos, incorporando las posibilidades de identificación y de firma electrónica de los mismos, y manteniendo la exigencia de exhibirlos a requerimiento de los agentes de la autoridad de conformidad con lo dispuesto en la Ley.

El capítulo III habilita a las autoridades competentes para acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación.

En este sentido, se regulan con detalle las facultades de las autoridades y de los agentes de las Fuerzas y Cuerpos de Seguridad para dictar órdenes e instrucciones, para la entrada y registro en domicilios, requerir la identificación de personas, efectuar comprobaciones y registros en lugares públicos, establecer restricciones del tránsito y controles en la vía pública, así como otras medidas extraordinarias en situaciones de emergencia imprescindible para garantizar la seguridad ciudadana (desalojo de locales o establecimientos, prohibición de paso, evacuación de inmuebles, etc.). Igualmente se regulan las medidas que deberán adoptar las autoridades para proteger la celebración de reuniones y manifestaciones, así como para restablecer la normalidad de su desarrollo en casos de alteración de la seguridad ciudadana.

La relación de estas potestades de policía de seguridad es análoga a la contenida en la Ley Orgánica 1/1992, de 21 de febrero, si bien, en garantía de los derechos de los ciudadanos que puedan verse afectados por su legítimo ejercicio por parte de los miembros de las Fuerzas y Cuerpos de Seguridad, se perfilan con mayor precisión los presupuestos habilitantes y las condiciones y requisitos de su ejercicio, de acuerdo con la jurisprudencia constitucional. Así, la habilitación a los agentes de las Fuerzas y Cuerpos de Seguridad para la práctica de identificaciones en la vía pública no se justifica genéricamente –como sucede en la Ley de 1992– en el ejercicio de las funciones de protección de la seguridad ciudadana, sino que es precisa la existencia de indicios de participación en la comisión de una infracción, o que razonablemente se considere necesario realizar la identificación para prevenir la comisión de un delito; por otra parte, en la práctica de esta diligencia, los agentes deberán respetar escrupulosamente los principios de proporcionalidad, igualdad de trato y no discriminación, y sólo en caso de negativa a la identificación, o si ésta no pudiera realizarse in situ, podrá requerirse a la persona para que acompañe a los agentes a las dependencias policiales más próximas en las que pueda efectuarse dicha identificación, informándola de modo inmediato y comprensible de los fines de la solicitud de identificación y, en su caso, de las razones del requerimiento.

Por primera vez se regulan los registros corporales externos, que sólo podrán realizarse cuando existan motivos para suponer que pueden conducir al hallazgo de instrumentos, efectos u otros objetos relevantes para el ejercicio de las funciones de indagación y prevención que encomiendan las Leyes a las Fuerzas y Cuerpos de Seguridad. Estos registros, de carácter superficial, deberán ocasionar el menor perjuicio a la dignidad de la persona, efectuarse por un agente del mismo sexo que la persona sobre la que se practique y, cuando lo exija el respeto a la intimidad, en un lugar reservado y fuera de la vista de terceros.

El capítulo IV, referente a las potestades especiales de la policía administrativa de seguridad, regula las medidas de control administrativo que el Estado puede ejercer sobre las actividades relacionadas con armas, explosivos, cartuchería y artículos pirotécnicos.

Asimismo, se establecen obligaciones de registro documental para actividades relevantes para la seguridad ciudadana, como el hospedaje, el acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público, la compraventa de joyas y metales, objetos u obras de arte, la cerrajería de seguridad o el comercio al por mayor de chatarra o productos de desecho.

Por otro lado, desde la estricta perspectiva de la seguridad ciudadana, se contempla el régimen de intervención de las autoridades competentes en materia de espectáculos públicos y actividades recreativas, sin perjuicio de las competencias de las comunidades autónomas y de las entidades locales en lo que se refiere a su normal desarrollo.

El capítulo V, que regula el régimen sancionador, introduce novedades relevantes con respecto a la Ley Orgánica 1/1992, de 21 de febrero. La redacción del capítulo en su conjunto tiene en cuenta, como reiteradamente ha declarado el Tribunal Constitucional, que el Derecho administrativo sancionador y el Derecho penal son, con matices, manifestaciones de un único ius puniendi del Estado. Por tanto, la Ley está orientada a dar cumplimiento a los principios que rigen la potestad sancionadora administrativa, singularmente los de responsabilidad, proporcionalidad y legalidad, en sus dos vertientes, de legalidad formal o reserva de Ley y legalidad material o tipicidad, sin perjuicio de la admisión de la colaboración reglamentaria para la especificación de conductas y sanciones en relación con las infracciones tipificadas por la Ley.

En cuanto a los autores de las conductas tipificadas como infracciones, se exime de responsabilidad a los menores de catorce años, en consonancia con la legislación sobre responsabilidad penal del menor. Asimismo se prevé que cuando sea declarado autor de los hechos cometidos un menor de dieciocho años no emancipado o una persona con la capacidad modificada judicialmente responderán solidariamente con él de los daños y perjuicios ocasionados sus padres, tutores, curadores, acogedores o guardadores legales o de hecho.

A fin de garantizar la proporcionalidad en la imposición de las sanciones graves y muy graves previstas en la Ley, se dividen las sanciones pecuniarias en tres tramos de igual extensión, que dan lugar a los grados mínimo, medio y máximo de las mismas y se recogen las circunstancias agravantes y los criterios de graduación que deberán tenerse en cuenta para la individualización de las sanciones pecuniarias, acogiendo así una exigencia del principio de proporcionalidad presente en la jurisprudencia contencioso-administrativa, pero que tiene escaso reflejo en los regímenes sancionadores que incorporan numerosas normas de nuestro ordenamiento jurídico administrativo.

Con respecto al cuadro de infracciones, en aras de un mejor ajuste al principio de tipicidad, se introduce un elenco de conductas que se califican como leves, graves y muy graves, estas últimas ausentes de la Ley Orgánica 1/1992, de 21 de febrero, que simplemente permitía la calificación de determinadas infracciones graves como muy graves en función de las circunstancias concurrentes.

Junto a las infracciones tipificadas por el legislador de 1992, la Ley sanciona conductas que, sin ser constitutivas de delito, atentan gravemente contra la seguridad ciudadana, como son las reuniones o manifestaciones prohibidas en lugares que tengan la condición de infraestructuras e instalaciones en las que se prestan servicios básicos para la comunidad y los actos de intrusión en éstas, cuando se ocasione un riesgo para las personas; la proyección de haces de luz sobre los conductores o pilotos de medios de transporte con riesgo de provocar un accidente, o la celebración de espectáculos públicos o actividades

recreativas a pesar de la prohibición o suspensión acordada por la autoridad por razones de seguridad, entre otras. Se sancionan igualmente conductas que representan un ejercicio extralimitado del derecho de reunión y manifestación, así como la perturbación del ejercicio de este derecho fundamental cuando no constituyan delito. Otras infracciones tienen por objeto preservar el legítimo ejercicio de sus funciones por las autoridades y sus agentes, así como por los servicios de emergencia.

Por otra parte, la reforma en tramitación del Código Penal exige una revisión de las infracciones penales de esta naturaleza que contenía el libro III del código punitivo para incorporar al ámbito administrativo algunas conductas que, de lo contrario, quedarían impunes, como son ciertas alteraciones del orden público, las faltas de respeto a la autoridad, el deslucimiento de determinados bienes en la vía pública o dejar sueltos animales peligrosos. También se recogen las infracciones previstas en la Ley Orgánica 1/1992, de 21 de febrero, relacionadas con el consumo de drogas tóxicas, estupefacientes o sustancias psicotrópicas, a las que se agregan otras dirigidas a favorecerlo. Se ha considerado oportuno sancionar comportamientos atentatorios a la libertad sexual de las personas, especialmente de los menores, o que perturban la convivencia ciudadana o el pacífico disfrute de las vías y espacios públicos, todos ellos bienes jurídicos cuya protección forma parte de los fines de esta Ley por su colindancia con la seguridad ciudadana.

Respecto de las sanciones, se reordenan las pecuniarias y se establecen tres tramos de igual extensión, que dan lugar a los grados mínimo, medio y máximo de las mismas, si bien no se eleva el importe de las que pueden imponerse por la comisión de infracciones muy graves, a pesar del tiempo transcurrido desde la aprobación de la Ley Orgánica 1/1992, de 21 de febrero. Asimismo se ha previsto que cabrá exigir al infractor, en su caso, la reposición de los bienes dañados a su situación originaria o, cuando ello no fuera posible, la indemnización por los daños y perjuicios causados, al igual que también sucede en otros ámbitos en los que se exige una reparación in natura de la situación alterada con el comportamiento infractor y, en su defecto, la satisfacción de un equivalente económico. Y con objeto de dar el tratamiento adecuado a las infracciones de los menores de dieciocho años en materia de consumo o tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas se prevé la suspensión de la sanción si aquéllos accedan a someterse a tratamiento o rehabilitación, si lo precisan, o a actividades reeducativas.

A fin de contribuir a evitar la proliferación de procedimientos administrativos especiales, se establece que el ejercicio de la potestad sancionadora en materia de protección de la seguridad ciudadana se regirá por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y su normativa de desarrollo, sin renunciar a la incorporación de determinadas especialidades, como la regulación de un procedimiento abreviado, que permite satisfacer el pago voluntario de las sanciones pecuniarias por la comisión de infracciones graves o leves en un breve plazo desde su notificación, con el efecto de la reducción del 50 por 100 de su importe, en términos análogos a los ya contemplados en otras normas. Se crea, en fin, un Registro Central de Infracciones contra la Seguridad Ciudadana, indispensable para poder apreciar la reincidencia de los infractores y permitir, de este modo, sancionar adecuadamente a quienes de modo voluntario y reiterado incurren en conductas merecedoras de reproche jurídico.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. La seguridad ciudadana es un requisito indispensable para el pleno ejercicio de los derechos fundamentales y las libertades públicas, y su salvaguarda, como bien jurídico de carácter colectivo, es función del Estado, con sujeción a la Constitución y a las Leyes.

2. Esta Ley tiene por objeto la regulación de un conjunto plural y diversificado de actuaciones de distinta naturaleza orientadas a la tutela de la seguridad ciudadana, mediante la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos.

Artículo 2. *Ámbito de aplicación.*

1. Las disposiciones de esta Ley son aplicables en todo el territorio nacional, sin perjuicio de las competencias que, en su caso, hayan asumido las comunidades autónomas en el marco de la Constitución, de los estatutos de autonomía y de la legislación del Estado en materia de seguridad pública.

2. En particular, quedan fuera del ámbito de aplicación de esta Ley las prescripciones que tienen por objeto velar por el buen orden de los espectáculos y la protección de las personas y bienes a través de una acción administrativa ordinaria, aun cuando la misma pueda conllevar la intervención de las Fuerzas y Cuerpos de Seguridad, siempre que ésta se conciba como elemento integrante del sistema preventivo habitual del control del espectáculo.

3. Asimismo, esta Ley se aplicará sin menoscabo de los regímenes legales que regulan ámbitos concretos de la seguridad pública, como la seguridad aérea, marítima, ferroviaria, vial o en los transportes, quedando, en todo caso, salvaguardadas las disposiciones referentes a la defensa nacional y la regulación de los estados de alarma, excepción y sitio.

Artículo 3. *Fines.*

Constituyen los fines de esta Ley y de la acción de los poderes públicos en su ámbito de aplicación:

a) La protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico.

b) La garantía del normal funcionamiento de las instituciones.

c) La preservación de la seguridad y la convivencia ciudadanas.

d) El respeto a las Leyes, a la paz y a la seguridad ciudadana en el ejercicio de los derechos y libertades.

e) La protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección.

f) La pacífica utilización de vías y demás bienes demaniales y, en general, espacios destinados al uso y disfrute público.

g) La garantía de las condiciones de normalidad en la prestación de los servicios básicos para la comunidad.

h) La prevención de la comisión de delitos e infracciones administrativas directamente relacionadas con los fines indicados en los párrafos anteriores y la sanción de las de esta naturaleza tipificadas en esta Ley.

i) La transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana.

Artículo 4. *Principios rectores de la acción de los poderes públicos en relación con la seguridad ciudadana.*

1. El ejercicio de las potestades y facultades reconocidas por esta Ley a las administraciones públicas y, específicamente, a las autoridades y demás órganos competentes en materia de seguridad ciudadana y a los miembros de las Fuerzas y Cuerpos de Seguridad se regirá por los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, y se someterá al control administrativo y jurisdiccional.

En particular, las disposiciones de los capítulos III y V deberán interpretarse y aplicarse del modo más favorable a la plena efectividad de los derechos fundamentales y libertades públicas, singularmente de los derechos de reunión y manifestación, las libertades de expresión e información, la libertad sindical y el derecho de huelga.

2. En particular, la actuación de los miembros de las Fuerzas y Cuerpos de Seguridad está sujeta a los principios básicos de actuación regulados en el artículo 5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

3. La actividad de intervención se justifica por la existencia de una amenaza concreta o de un comportamiento objetivamente peligroso que, razonablemente, sea susceptible de provocar un perjuicio real para la seguridad ciudadana y, en concreto, atentar contra los

derechos y libertades individuales y colectivos o alterar el normal funcionamiento de las instituciones públicas. Las concretas intervenciones para el mantenimiento y restablecimiento de la seguridad ciudadana se realizarán conforme a lo dispuesto en el capítulo III de esta Ley.

Artículo 5. *Autoridades y órganos competentes.*

1. Corresponde al Gobierno, a través del Ministerio del Interior y de los demás órganos y autoridades competentes y de las Fuerzas y Cuerpos de Seguridad a sus órdenes, la preparación, dirección y ejecución de la política en relación con la administración general de la seguridad ciudadana, sin perjuicio de las competencias atribuidas a otras administraciones públicas en dicha materia.

2. Son autoridades y órganos competentes en materia de seguridad ciudadana, en el ámbito de la Administración General del Estado:

a) El Ministro del Interior.

b) El Secretario de Estado de Seguridad.

c) Los titulares de los órganos directivos del Ministerio del Interior que tengan atribuida tal condición, en virtud de disposiciones legales o reglamentarias.

d) Los Delegados del Gobierno en las comunidades autónomas y en las Ciudades de Ceuta y Melilla.

e) Los Subdelegados del Gobierno en las provincias y los Directores Insulares.

3. Serán autoridades y órganos competentes, a los efectos de esta Ley, los correspondientes de las comunidades autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio.

4. Las autoridades de las Ciudades de Ceuta y Melilla y las autoridades locales ejercerán las facultades que les corresponden, de acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, y la legislación de régimen local, espectáculos públicos, actividades recreativas y actividades clasificadas.

Artículo 6. *Cooperación interadministrativa.*

La Administración General del Estado y las demás administraciones públicas con competencias en materia de seguridad ciudadana se regirán, en sus relaciones, por los principios de cooperación y lealtad institucional, facilitándose la información de acuerdo con la legislación vigente y la asistencia técnica necesarias en el ejercicio de sus respectivas atribuciones, y, cuando fuese preciso, coordinando las acciones destinadas a garantizar el cumplimiento de esta Ley, de conformidad con lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 7. *Deber de colaboración.*

1. Todas las autoridades y funcionarios públicos, en el ámbito de sus respectivas competencias y de acuerdo con su normativa específica, deberán colaborar con las autoridades y órganos a que se refiere el artículo 5, y prestarles el auxilio que sea posible y adecuado para la consecución de los fines relacionados en el artículo 3. Cuando, por razón de su cargo, tengan conocimiento de hechos que perturben gravemente la seguridad ciudadana o de los que racionalmente pueda inferirse que pueden producir una perturbación grave, estarán obligados a ponerlo inmediatamente en conocimiento de la autoridad competente.

2. Las autoridades y órganos competentes y los miembros de las Fuerzas y Cuerpos de Seguridad podrán recabar de los particulares su ayuda y colaboración en la medida necesaria para el cumplimiento de los fines previstos en esta Ley, especialmente en los casos de grave calamidad pública o catástrofe extraordinaria, siempre que ello no implique riesgo personal para los mismos. Quienes sufran daños y perjuicios por estas causas serán indemnizados de acuerdo con las leyes.

3. Las empresas de seguridad privada, los despachos de detectives privados y el personal de seguridad privada tienen un especial deber de auxiliar a las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones, prestarles la colaboración que precisen y seguir sus instrucciones, en los términos previstos en la normativa de seguridad privada.

4. El personal que realice funciones de policía administrativa tendrá el especial deber de colaborar en la consecución de los fines previstos en el artículo 3 de esta Ley.

CAPÍTULO II

Documentación e identificación personal

Artículo 8. *Acreditación de la identidad de los ciudadanos españoles.*

1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a éstos otorgan las leyes, así como suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular.

2. En el Documento Nacional de Identidad figurarán la fotografía y la firma de su titular, así como los datos personales que se determinen reglamentariamente, que respetarán el derecho a la intimidad de la persona, sin que en ningún caso, puedan ser relativos a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. La tarjeta soporte del Documento Nacional de Identidad incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación.

3. El Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica. Las personas con capacidad modificada judicialmente podrán ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar.

El prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona.

Artículo 9. *Obligaciones y derechos del titular del Documento Nacional de Identidad.*

1. El Documento Nacional de Identidad es obligatorio a partir de los catorce años. Dicho documento es personal e intransferible, debiendo su titular mantenerlo en vigor y conservarlo y custodiarlo con la debida diligencia. No podrá ser privado del mismo, ni siquiera temporalmente, sino en los supuestos en que, conforme a lo previsto por la ley, haya de ser sustituido por otro documento.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo y permitir la comprobación de las medidas de seguridad a las que se refiere el apartado 2 del artículo 8 cuando fueren requeridas para ello por la autoridad o sus agentes, para el cumplimiento de los fines previstos en el apartado 1 del artículo 16. De su sustracción o extravío deberá darse cuenta tan pronto como sea posible a la comisaría de Policía o puesto de las Fuerzas y Cuerpos de Seguridad más próximo.

Artículo 10. *Competencias sobre el Documento Nacional de Identidad.*

1. Corresponde al Ministerio del Interior la competencia exclusiva para la dirección, organización y gestión de todos los aspectos referentes a la confección y expedición del Documento Nacional de Identidad, conforme a lo dispuesto en esta Ley y en la legislación sobre firma electrónica.

2. La competencia a que se refiere el apartado anterior será ejercida por la Dirección General de la Policía, a la que corresponderá también la custodia y responsabilidad de los archivos y ficheros relacionados con el Documento Nacional de Identidad.

3. Su expedición está sujeta al pago de una tasa.

Artículo 11. *Pasaporte de ciudadanos españoles.*

1. El pasaporte español es un documento público, personal, individual e intransferible que, salvo prueba en contrario, acredita la identidad y nacionalidad de los ciudadanos españoles fuera de España, y dentro del territorio nacional, las mismas circunstancias de los españoles no residentes.

2. Los ciudadanos españoles tienen derecho a que les sea expedido el pasaporte, que sólo podrá ser exceptuado en las siguientes circunstancias:

a) Haber sido condenado a penas o medidas de seguridad privativas de libertad, mientras no se hayan extinguido, salvo que obtenga autorización del órgano judicial competente.

b) Haber sido acordada por el órgano judicial competente la retirada de su pasaporte de acuerdo con lo previsto por la ley.

c) Haberle sido impuesta una medida de libertad vigilada con prohibición de abandonar el territorio nacional, salvo que obtenga autorización del órgano judicial competente.

d) Cuando el órgano judicial competente haya prohibido la salida de España o la expedición de pasaporte al menor de edad o a la persona con la capacidad modificada judicialmente, de acuerdo con lo dispuesto por la ley.

3. La obtención del pasaporte por los ciudadanos sujetos a patria potestad o a tutela estará condicionada al consentimiento expreso de las personas u órgano que tenga encomendado su ejercicio o, en su defecto, del órgano judicial competente.

4. Los titulares del pasaporte tienen la obligación de exhibirlo y facilitarlo cuando fuesen requeridos para ello por la autoridad o sus agentes. También estarán obligados a su custodia y conservación con la debida diligencia. De su sustracción o extravío deberá darse cuenta de manera inmediata a las Fuerzas y Cuerpos de Seguridad o, en su caso, a la Representación Diplomática o Consular de España en el extranjero.

Artículo 12. *Competencias sobre el pasaporte.*

1. La competencia para su expedición corresponde:

a) En el territorio nacional, a la Dirección General de la Policía.

b) En el extranjero, a las Representaciones Diplomáticas y Consulares de España.

2. Su expedición está sujeta al pago de una tasa.

3. Corresponde al Gobierno, a propuesta de los Ministros del Interior y de Asuntos Exteriores y de Cooperación, desarrollar esta Ley en lo referente al régimen jurídico del pasaporte.

Artículo 13. *Acreditación de la identidad de ciudadanos extranjeros.*

1. Los extranjeros que se encuentren en territorio español tienen el derecho y la obligación de conservar y portar consigo la documentación que acredite su identidad expedida por las autoridades competentes del país de origen o de procedencia, así como la que acredite su situación regular en España.

2. Los extranjeros no podrán ser privados de su documentación de origen, salvo en el curso de investigaciones judiciales de carácter penal.

3. Los extranjeros estarán obligados a exhibir la documentación mencionada en el apartado 1 de este artículo y permitir la comprobación de las medidas de seguridad de la misma, cuando fueran requeridos por las autoridades o sus agentes de conformidad con lo dispuesto en la ley, y por el tiempo imprescindible para dicha comprobación, sin perjuicio de poder demostrar su identidad por cualquier otro medio si no la llevaran consigo.

CAPÍTULO III

Actuaciones para el mantenimiento y restablecimiento de la seguridad ciudadana

Sección 1.ª Potestades generales de policía de seguridad

Artículo 14. *Órdenes y prohibiciones.*

Las autoridades competentes, de conformidad con las Leyes y reglamentos, podrán dictar las órdenes y prohibiciones y disponer las actuaciones policiales estrictamente necesarias para asegurar la consecución de los fines previstos en esta Ley, mediante resolución debidamente motivada.

Artículo 15. *Entrada y registro en domicilio y edificios de organismos oficiales.*

1. Los agentes de las Fuerzas y Cuerpos de Seguridad sólo podrán proceder a la entrada y registro en domicilio en los casos permitidos por la Constitución y en los términos que fijen las Leyes.

2. Será causa legítima suficiente para la entrada en domicilio la necesidad de evitar daños inminentes y graves a las personas y a las cosas, en supuestos de catástrofe, calamidad, ruina inminente u otros semejantes de extrema y urgente necesidad.

3. Para la entrada en edificios ocupados por organismos oficiales o entidades públicas, no será preciso el consentimiento de la autoridad o funcionario que los tuviere a su cargo.

4. Cuando por las causas previstas en este artículo las Fuerzas y Cuerpos de Seguridad entren en un domicilio particular, remitirán sin dilación el acta o atestado que instruyan a la autoridad judicial competente.

Artículo 16. *Identificación de personas.*

1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:

a) Cuando existan indicios de que han podido participar en la comisión de una infracción.

b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito.

En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados.

En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social.

2. Cuando no fuera posible la identificación por cualquier medio, incluida la vía telemática o telefónica, o si la persona se negase a identificarse, los agentes, para impedir la comisión de un delito o al objeto de sancionar una infracción, podrán requerir a quienes no pudieran ser identificados a que les acompañen a las dependencias policiales más próximas en las que se disponga de los medios adecuados para la práctica de esta diligencia, a los solos efectos de su identificación y por el tiempo estrictamente necesario, que en ningún caso podrá superar las seis horas.

La persona a la que se solicite que se identifique será informada de modo inmediato y comprensible de las razones de dicha solicitud, así como, en su caso, del requerimiento para que acompañe a los agentes a las dependencias policiales.

3. En las dependencias a que se hace referencia en el apartado 2 se llevará un libro-registro en el que sólo se practicarán asientos relacionados con la seguridad ciudadana. Constarán en él las diligencias de identificación practicadas, así como los motivos, circunstancias y duración de las mismas, y sólo podrán ser comunicados sus datos a la autoridad judicial competente y al Ministerio Fiscal. El órgano competente de la Administración remitirá mensualmente al Ministerio Fiscal extracto de las diligencias de identificación con expresión del tiempo utilizado en cada una. Los asientos de este libro-registro se cancelarán de oficio a los tres años.

4. A las personas desplazadas a dependencias policiales a efectos de identificación, se les deberá expedir a su salida un volante acreditativo del tiempo de permanencia en ellas, la causa y la identidad de los agentes actuantes.

5. En los casos de resistencia o negativa a identificarse o a colaborar en las comprobaciones o prácticas de identificación, se estará a lo dispuesto en el Código Penal, en la Ley de Enjuiciamiento Criminal y, en su caso, en esta Ley.

Artículo 17. *Restricción del tránsito y controles en las vías públicas.*

1. Los agentes de las Fuerzas y Cuerpos de Seguridad podrán limitar o restringir la circulación o permanencia en vías o lugares públicos y establecer zonas de seguridad en supuestos de alteración de la seguridad ciudadana o de la pacífica convivencia, o cuando existan indicios racionales de que pueda producirse dicha alteración, por el tiempo imprescindible para su mantenimiento o restablecimiento. Asimismo podrán ocupar preventivamente los efectos o instrumentos susceptibles de ser utilizados para acciones ilegales, dándoles el destino que legalmente proceda.

2. Para la prevención de delitos de especial gravedad o generadores de alarma social, así como para el descubrimiento y detención de quienes hubieran participado en su comisión y proceder a la recogida de los instrumentos, efectos o pruebas, se podrán establecer controles en las vías, lugares o establecimientos públicos, siempre que resulte indispensable proceder a la identificación de personas que se encuentren en ellos, al registro de vehículos o al control superficial de efectos personales.

Artículo 18. *Comprobaciones y registros en lugares públicos.*

1. Los agentes de la autoridad podrán practicar las comprobaciones en las personas, bienes y vehículos que sean necesarias para impedir que en las vías, lugares y establecimientos públicos se porten o utilicen ilegalmente armas, explosivos, sustancias peligrosas u otros objetos, instrumentos o medios que generen un riesgo potencialmente grave para las personas, susceptibles de ser utilizados para la comisión de un delito o alterar la seguridad ciudadana, cuando tengan indicios de su eventual presencia en dichos lugares, procediendo, en su caso, a su intervención. A tal fin, los ciudadanos tienen el deber de colaborar y no obstaculizar la labor de los agentes de la autoridad en el ejercicio de sus funciones.

2. Los agentes de la autoridad podrán proceder a la ocupación temporal de cualesquiera objetos, instrumentos o medios de agresión, incluso de las armas que se porten con licencia, permiso o autorización si se estima necesario, con objeto de prevenir la comisión de cualquier delito, o cuando exista peligro para la seguridad de las personas o de los bienes.

Artículo 19. *Disposiciones comunes a las diligencias de identificación, registro y comprobación.*

1. Las diligencias de identificación, registro y comprobación practicadas por los agentes de las Fuerzas y Cuerpos de Seguridad con ocasión de actuaciones realizadas conforme a lo dispuesto en esta sección no estarán sujetas a las mismas formalidades que la detención.

2. La aprehensión durante las diligencias de identificación, registro y comprobación de armas, drogas tóxicas, estupefacientes, sustancias psicotrópicas u otros efectos procedentes de un delito o infracción administrativa se hará constar en el acta correspondiente, que habrá de ser firmada por el interesado; si éste se negara a firmarla, se dejará constancia expresa de su negativa. El acta que se extienda gozará de presunción de veracidad de los hechos en ella consignados, salvo prueba en contrario.

Artículo 20. *Registros corporales externos.*

1. Podrá practicarse el registro corporal externo y superficial de la persona cuando existan indicios racionales para suponer que puede conducir al hallazgo de instrumentos, efectos u otros objetos relevantes para el ejercicio de las funciones de indagación y prevención que encomiendan las leyes a las Fuerzas y Cuerpos de Seguridad.

2. Salvo que exista una situación de urgencia por riesgo grave e inminente para los agentes:

a) El registro se realizará por un agente del mismo sexo que la persona sobre la que se practique esta diligencia.

b) Y si exigiera dejar a la vista partes del cuerpo normalmente cubiertas por ropa, se efectuará en un lugar reservado y fuera de la vista de terceros. Se dejará constancia escrita de esta diligencia, de sus causas y de la identidad del agente que la adoptó.

3. Los registros corporales externos respetarán los principios del apartado 1 del artículo 16, así como el de injerencia mínima, y se realizarán del modo que cause el menor perjuicio a la intimidad y dignidad de la persona afectada, que será informada de modo inmediato y comprensible de las razones de su realización.

4. Los registros a los que se refiere este artículo podrán llevarse a cabo contra la voluntad del afectado, adoptando las medidas de compulsión indispensables, conforme a los principios de idoneidad, necesidad y proporcionalidad.

Artículo 21. *Medidas de seguridad extraordinarias.*

Las autoridades competentes podrán acordar, como medidas de seguridad extraordinarias, el cierre o desalojo de locales o establecimientos, la prohibición del paso, la evacuación de inmuebles o espacios públicos debidamente acotados, o el depósito de explosivos u otras sustancias susceptibles de ser empleadas como tales, en situaciones de emergencia que las hagan imprescindibles y durante el tiempo estrictamente necesario para garantizar la seguridad ciudadana. Dichas medidas podrán adoptarse por los agentes de la autoridad si la urgencia de la situación lo hiciera imprescindible, incluso mediante órdenes verbales.

A los efectos de este artículo, se entiende por emergencia aquella situación de riesgo sobrevenida por un evento que pone en peligro inminente a personas o bienes y exige una actuación rápida por parte de la autoridad o de sus agentes para evitarla o mitigar sus efectos.

Artículo 22. *Uso de videocámaras.*

La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.

Sección 2.ª Mantenimiento y restablecimiento de la seguridad ciudadana en reuniones y manifestaciones

Artículo 23. *Reuniones y manifestaciones.*

1. Las autoridades a las que se refiere esta Ley adoptarán las medidas necesarias para proteger la celebración de reuniones y manifestaciones, impidiendo que se perturbe la seguridad ciudadana.

Asimismo podrán acordar la disolución de reuniones en lugares de tránsito público y manifestaciones en los supuestos previstos en el artículo 5 de la Ley Orgánica 9/1983, de 15 de julio, reguladora del derecho de reunión.

También podrán disolver las concentraciones de vehículos en las vías públicas y retirar aquéllos o cualesquiera otra clase de obstáculos cuando impidieran, pusieran en peligro o dificultaran la circulación por dichas vías.

2. Las medidas de intervención para el mantenimiento o el restablecimiento de la seguridad ciudadana en reuniones y manifestaciones serán graduales y proporcionadas a las circunstancias. La disolución de reuniones y manifestaciones constituirá el último recurso.

3. Antes de adoptar las medidas a las que se refiere el apartado anterior, las unidades actuantes de las Fuerzas y Cuerpos de Seguridad deberán avisar de tales medidas a las personas afectadas, pudiendo hacerlo de manera verbal si la urgencia de la situación lo hiciera imprescindible.

En caso de que se produzca una alteración de la seguridad ciudadana con armas, artefactos explosivos u objetos contundentes o de cualquier otro modo peligrosos, las Fuerzas y Cuerpos de Seguridad podrán disolver la reunión o manifestación o retirar los vehículos y obstáculos sin necesidad de previo aviso.

Artículo 24. *Colaboración entre las Fuerzas y Cuerpos de Seguridad.*

En los casos a que se refiere el artículo anterior, las Fuerzas y Cuerpos de Seguridad colaborarán mutuamente en los términos previstos en su Ley orgánica reguladora.

CAPÍTULO IV

Potestades especiales de policía administrativa de seguridad

Artículo 25. *Obligaciones de registro documental.*

1. Las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, como las de hospedaje, transporte de personas, acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público, comercio o reparación de objetos usados, alquiler o desguace de vehículos de motor, compraventa de joyas y metales, ya sean preciosos o no, objetos u obras de arte, cerrajería de seguridad, centros gestores de residuos metálicos, establecimientos de comercio al por mayor de chatarra o productos de desecho, o de venta de productos químicos peligrosos a particulares, quedarán sujetas a las obligaciones de registro documental e información en los términos que establezcan las disposiciones aplicables.

2. Los titulares de embarcaciones de alta velocidad, así como los de aeronaves ligeras estarán obligados a realizar las actuaciones de registro documental e información previstas en la normativa vigente.

Artículo 26. *Establecimientos e instalaciones obligados a adoptar medidas de seguridad.*

Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables.

Artículo 27. *Espectáculos y actividades recreativas.*

1. El Estado podrá dictar normas de seguridad pública para los edificios e instalaciones en los que se celebren espectáculos y actividades recreativas.

2. Las autoridades a las que se refiere esta Ley adoptarán las medidas necesarias para preservar la pacífica celebración de espectáculos públicos. En particular, podrán prohibir y, en caso de estar celebrándose, suspender los espectáculos y actividades recreativas cuando exista un peligro cierto para personas y bienes, o acaecieran o se previeran graves alteraciones de la seguridad ciudadana.

3. La normativa específica determinará los supuestos en los que los delegados de la autoridad deban estar presentes en la celebración de los espectáculos y actividades recreativas, los cuales podrán proceder, previo aviso a los organizadores, a la suspensión de los mismos por razones de máxima urgencia en los supuestos previstos en el apartado anterior.

4. Los espectáculos deportivos quedarán, en todo caso, sujetos a las medidas de prevención de la violencia dispuestas en la legislación específica contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

Artículo 28. *Control administrativo sobre armas, explosivos, cartuchería y artículos pirotécnicos.*

1. Corresponde al Gobierno:

a) La regulación de los requisitos y condiciones de fabricación, reparación, circulación, almacenamiento, comercio, adquisición, enajenación, tenencia y utilización de armas, sus imitaciones, réplicas y piezas fundamentales.

b) La regulación de los requisitos y condiciones mencionados anteriormente en relación con los explosivos, cartuchería y artículos pirotécnicos.

c) La adopción de las medidas de control necesarias para el cumplimiento de los requisitos y condiciones a que se refieren los párrafos a) y b).

2. La intervención de armas, explosivos, cartuchería y artículos pirotécnicos corresponde al Ministerio del Interior, que la ejerce a través de la Dirección General de la Guardia Civil, cuyos servicios están habilitados para realizar en cualquier momento las inspecciones y comprobaciones que sean necesarias en los espacios que estén destinados a su fabricación, depósito, comercialización o utilización.

Artículo 29. *Medidas de control.*

1. El Gobierno regulará las medidas de control necesarias sobre las materias relacionadas en el artículo anterior:

a) Mediante la sujeción de la apertura y funcionamiento de las fábricas, talleres, depósitos, establecimientos de comercialización y lugares de utilización y las actividades relacionadas con ellas a requisitos de catalogación o clasificación, autorización, información, inspección, vigilancia y control, requisitos especiales de habilitación para el personal encargado de su manipulación, así como la determinación del régimen de responsabilidad de quienes tengan el deber de prevenir la comisión de determinadas infracciones.

b) Estableciendo la obligatoria titularidad de licencias, permisos o autorizaciones para la adquisición, tenencia y utilización de armas de fuego, cuya expedición tendrá carácter restrictivo cuando se trate de armas de defensa personal, en relación con las cuales la concesión de las licencias, permisos o autorizaciones se limitará a supuestos de estricta necesidad. Para la concesión de licencias, permisos y autorizaciones se tendrán en cuenta la conducta y antecedentes del interesado. En todo caso, el solicitante prestará su consentimiento expreso a favor del órgano de la Administración General del Estado que tramita su solicitud para que se recaben sus antecedentes penales.

c) A través de la prohibición de la fabricación, tenencia y comercialización de armas, cartuchería, artículos pirotécnicos y explosivos especialmente peligrosos, así como el depósito de los mismos.

2. La fabricación, comercio y distribución de armas, artículos pirotécnicos, cartuchería y explosivos, constituye un sector con regulación específica en materia de derecho de establecimiento, en los términos previstos por la legislación sobre inversiones extranjeras en España, correspondiendo a los Ministerios de Defensa, del Interior y de Industria, Energía y Turismo el ejercicio de las competencias de supervisión y control.

CAPÍTULO V

Régimen sancionador

Sección 1.ª Sujetos responsables, órganos competentes y reglas generales sobre las infracciones y la aplicación de las sanciones

Artículo 30. *Sujetos responsables.*

1. La responsabilidad por las infracciones cometidas recaerá directamente en el autor del hecho en que consista la infracción.

2. Estarán exentos de responsabilidad por las infracciones cometidas los menores de catorce años.

En caso de que la infracción sea cometida por un menor de catorce años, la autoridad competente lo pondrá en conocimiento del Ministerio Fiscal para que inicie, en su caso, las actuaciones oportunas.

3. A los efectos de esta Ley se considerarán organizadores o promotores de las reuniones en lugares de tránsito público o manifestaciones las personas físicas o jurídicas que hayan suscrito la preceptiva comunicación. Asimismo, aun no habiendo suscrito o presentado la comunicación, también se considerarán organizadores o promotores quienes de hecho las presidan, dirijan o ejerzan actos semejantes, o quienes por publicaciones o declaraciones de convocatoria de las mismas, por las manifestaciones orales o escritas que en ellas se difundan, por los lemas, banderas u otros signos que ostenten o por cualesquiera otros hechos pueda determinarse razonablemente que son directores de aquellas.

Artículo 31. *Normas concursales.*

1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.

b) El precepto más amplio o complejo absorberá el que sancione las infracciones consumidas en aquel.

c) En defecto de los criterios anteriores, el precepto más grave excluirá los que sancionen el hecho con una sanción menor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que aplique una mayor sanción.

3. Cuando una acción u omisión deba tomarse en consideración como criterio de graduación de la sanción o como circunstancia que determine la calificación de la infracción no podrá ser sancionada como infracción independiente.

Artículo 32. *Órganos competentes.*

1. Son órganos competentes en el ámbito de la Administración General del Estado:

a) El Ministro del Interior, para la sanción de las infracciones muy graves en grado máximo.

b) El Secretario de Estado de Seguridad, para la sanción de infracciones muy graves en grado medio y en grado mínimo.

c) Los Delegados del Gobierno en las comunidades autónomas y en las Ciudades de Ceuta y Melilla, para la sanción de las infracciones graves y leves.

2. Serán competentes para imponer las sanciones tipificadas en esta Ley las autoridades correspondientes de la Comunidad Autónoma en el ámbito de sus competencias en materia de seguridad ciudadana.

3. Los alcaldes podrán imponer las sanciones y adoptar las medidas previstas en esta Ley cuando las infracciones se cometieran en espacios públicos municipales o afecten a

bienes de titularidad local, siempre que ostenten competencia sobre la materia de acuerdo con la legislación específica.

En los términos del artículo 41, las ordenanzas municipales podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones tipificadas en esta Ley.

Artículo 33. *Graduación de las sanciones.*

1. En la imposición de las sanciones por la comisión de las infracciones tipificadas en esta Ley se observará el principio de proporcionalidad, de acuerdo con lo dispuesto en los apartados siguientes.

2. Dentro de los límites previstos para las infracciones muy graves y graves, las multas se dividirán en tres tramos de igual extensión, correspondientes a los grados mínimo, medio y máximo, en los términos del apartado 1 del artículo 39.

La comisión de una infracción determinará la imposición de la multa correspondiente en grado mínimo.

La infracción se sancionará con multa en grado medio cuando se acredite la concurrencia, al menos, de una de las siguientes circunstancias:

a) La reincidencia, por la comisión en el término de dos años de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.

b) La realización de los hechos interviniendo violencia, amenaza o intimidación.

c) La ejecución de los hechos usando cualquier tipo de prenda u objeto que cubra el rostro, impidiendo o dificultando la identificación.

d) Que en la comisión de la infracción se utilice a menores de edad, personas con discapacidad necesitadas de especial protección o en situación de vulnerabilidad.

En cada grado, para la individualización de la multa se tendrán en cuenta los siguientes criterios:

a) La entidad del riesgo producido para la seguridad ciudadana o la salud pública.

b) La cuantía del perjuicio causado.

c) La trascendencia del perjuicio para la prevención, mantenimiento o restablecimiento de la seguridad ciudadana.

d) La alteración ocasionada en el funcionamiento de los servicios públicos o en el abastecimiento a la población de bienes y servicios.

e) El grado de culpabilidad.

f) El beneficio económico obtenido como consecuencia de la comisión de la infracción.

g) La capacidad económica del infractor.

Las infracciones sólo se sancionarán con multa en grado máximo cuando los hechos revistan especial gravedad y así se justifique teniendo en cuenta el número y la entidad de las circunstancias concurrentes y los criterios previstos en este apartado.

3. La multa por la comisión de infracciones leves se determinará directamente atendiendo a las circunstancias y los criterios del apartado anterior.

Sección 2.ª Infracciones y sanciones

Artículo 34. *Clasificación de las infracciones.*

Las infracciones tipificadas en esta Ley se clasifican en muy graves, graves y leves.

Artículo 35. *Infracciones muy graves.*

Son infracciones muy graves:

1. Las reuniones o manifestaciones no comunicadas o prohibidas en infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad o en sus inmediaciones, así como la intrusión en los recintos de éstas, incluido su sobrevuelo,

cuando, en cualquiera de estos supuestos, se haya generado un riesgo para la vida o la integridad física de las personas.

En el caso de las reuniones y manifestaciones serán responsables los organizadores o promotores.

2. La fabricación, reparación, almacenamiento, circulación, comercio, transporte, distribución, adquisición, certificación, enajenación o utilización de armas reglamentarias, explosivos catalogados, cartuchería o artículos pirotécnicos, incumpliendo la normativa de aplicación, careciendo de la documentación o autorización requeridas o excediendo los límites autorizados cuando tales conductas no sean constitutivas de delito así como la omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias, siempre que en tales actuaciones se causen perjuicios muy graves.

3. La celebración de espectáculos públicos o actividades recreativas quebrantando la prohibición o suspensión ordenada por la autoridad correspondiente por razones de seguridad pública.

4. La proyección de haces de luz, mediante cualquier tipo de dispositivo, sobre los pilotos o conductores de medios de transporte que puedan deslumbrarles o distraer su atención y provocar accidentes.

Artículo 36. *Infracciones graves.*

Son infracciones graves:

1. La perturbación de la seguridad ciudadana en actos públicos, espectáculos deportivos o culturales, solemnidades y oficios religiosos u otras reuniones a las que asistan numerosas personas, cuando no sean constitutivas de infracción penal.

2. La perturbación grave de la seguridad ciudadana que se produzca con ocasión de reuniones o manifestaciones frente a las sedes del Congreso de los Diputados, el Senado y las asambleas legislativas de las comunidades autónomas, aunque no estuvieran reunidas, cuando no constituya infracción penal.

3. Causar desórdenes en las vías, espacios o establecimientos públicos, u obstaculizar la vía pública con mobiliario urbano, vehículos, contenedores, neumáticos u otros objetos, cuando en ambos casos se ocasione una alteración grave de la seguridad ciudadana.

4. Los actos de obstrucción que pretendan impedir a cualquier autoridad, empleado público o corporación oficial el ejercicio legítimo de sus funciones, el cumplimiento o la ejecución de acuerdos o resoluciones administrativas o judiciales, siempre que se produzcan al margen de los procedimientos legalmente establecidos y no sean constitutivos de delito.

5. Las acciones y omisiones que impidan u obstaculicen el funcionamiento de los servicios de emergencia, provocando o incrementando un riesgo para la vida o integridad de las personas o de daños en los bienes, o agravando las consecuencias del suceso que motive la actuación de aquéllos.

6. La desobediencia o la resistencia a la autoridad o a sus agentes en el ejercicio de sus funciones, cuando no sean constitutivas de delito, así como la negativa a identificarse a requerimiento de la autoridad o de sus agentes o la alegación de datos falsos o inexactos en los procesos de identificación.

7. La negativa a la disolución de reuniones y manifestaciones en lugares de tránsito público ordenada por la autoridad competente cuando concurran los supuestos del artículo 5 de la Ley Orgánica 9/1983, de 15 de julio.

8. La perturbación del desarrollo de una reunión o manifestación lícita, cuando no constituya infracción penal.

9. La intrusión en infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad, incluyendo su sobrevuelo, cuando se haya producido una interferencia grave en su funcionamiento.

10. Portar, exhibir o usar armas prohibidas, así como portar, exhibir o usar armas de modo negligente, temerario o intimidatorio, o fuera de los lugares habilitados para su uso, aún cuando en este último caso se tuviera licencia, siempre que dichas conductas no constituyan infracción penal.

11. La solicitud o aceptación por el demandante de servicios sexuales retribuidos en zonas de tránsito público en las proximidades de lugares destinados a su uso por menores,

como centros educativos, parques infantiles o espacios de ocio accesibles a menores de edad, o cuando estas conductas, por el lugar en que se realicen, puedan generar un riesgo para la seguridad vial.

Los agentes de la autoridad requerirán a las personas que ofrezcan estos servicios para que se abstengan de hacerlo en dichos lugares, informándoles de que la inobservancia de dicho requerimiento podría constituir una infracción del párrafo 6 de este artículo.

12. La fabricación, reparación, almacenamiento, circulación, comercio, transporte, distribución, adquisición, certificación, enajenación o utilización de armas reglamentarias, explosivos catalogados, cartuchería o artículos pirotécnicos, incumpliendo la normativa de aplicación, careciendo de la documentación o autorización requeridas o excediendo los límites autorizados cuando tales conductas no sean constitutivas de delito, así como la omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias.

13. La negativa de acceso o la obstrucción deliberada de las inspecciones o controles reglamentarios, establecidos conforme a lo dispuesto en esta Ley, en fábricas, locales, establecimientos, embarcaciones y aeronaves.

14. El uso público e indebido de uniformes, insignias o condecoraciones oficiales, o réplicas de los mismos, así como otros elementos del equipamiento de los cuerpos policiales o de los servicios de emergencia que puedan generar engaño acerca de la condición de quien los use, cuando no sea constitutivo de infracción penal.

15. La falta de colaboración con las Fuerzas y Cuerpos de Seguridad en la averiguación de delitos o en la prevención de acciones que puedan poner en riesgo la seguridad ciudadana en los supuestos previstos en el artículo 7.

16. El consumo o la tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas, aunque no estuvieran destinadas al tráfico, en lugares, vías, establecimientos públicos o transportes colectivos, así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares.

17. El traslado de personas, con cualquier tipo de vehículo, con el objeto de facilitar a éstas el acceso a drogas tóxicas, estupefacientes o sustancias psicotrópicas, siempre que no constituya delito.

18. La ejecución de actos de plantación y cultivo ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas en lugares visibles al público, cuando no sean constitutivos de infracción penal.

19. La tolerancia del consumo ilegal o el tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas en locales o establecimientos públicos o la falta de diligencia en orden a impedirlos por parte de los propietarios, administradores o encargados de los mismos.

20. La carencia de los registros previstos en esta Ley para las actividades con trascendencia para la seguridad ciudadana o la omisión de comunicaciones obligatorias.

21. La alegación de datos o circunstancias falsos para la obtención de las documentaciones previstas en esta Ley, siempre que no constituya infracción penal.

22. El incumplimiento de las restricciones a la navegación reglamentariamente impuestas a las embarcaciones de alta velocidad y aeronaves ligeras.

23. El uso no autorizado de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información.

Artículo 37. *Infracciones leves.*

Son infracciones leves:

1. La celebración de reuniones en lugares de tránsito público o de manifestaciones, incumpliendo lo preceptuado en los artículos 4.2, 8, 9, 10 y 11 de la Ley Orgánica 9/1983, de 15 de julio, cuya responsabilidad corresponderá a los organizadores o promotores.

2. La exhibición de objetos peligrosos para la vida e integridad física de las personas con ánimo intimidatorio, siempre que no constituya delito o infracción grave.

3. El incumplimiento de las restricciones de circulación peatonal o itinerario con ocasión de un acto público, reunión o manifestación, cuando provoquen alteraciones menores en el normal desarrollo de los mismos.

4. Las faltas de respeto y consideración cuyo destinatario sea un miembro de las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones de protección de la seguridad, cuando estas conductas no sean constitutivas de infracción penal.

5. La realización o incitación a la realización de actos que atenten contra la libertad e indemnidad sexual, o ejecutar actos de exhibición obscena, cuando no constituya infracción penal.

6. La proyección de haces de luz, mediante cualquier tipo de dispositivo, sobre miembros de las Fuerzas y Cuerpos de Seguridad para impedir o dificultar el ejercicio de sus funciones.

7. La ocupación de cualquier inmueble, vivienda o edificio ajenos, o la permanencia en ellos, en ambos casos contra la voluntad de su propietario, arrendatario o titular de otro derecho sobre el mismo, cuando no sean constitutivas de infracción penal.

Asimismo la ocupación de la vía pública con infracción de lo dispuesto por la Ley o contra la decisión adoptada en aplicación de aquella por la autoridad competente. Se entenderá incluida en este supuesto la ocupación de la vía pública para la venta ambulante no autorizada.

8. La omisión o la insuficiencia de medidas para garantizar la conservación de la documentación de armas y explosivos, así como la falta de denuncia de la pérdida o sustracción de la misma.

9. Las irregularidades en la cumplimentación de los registros previstos en esta Ley con trascendencia para la seguridad ciudadana, incluyendo la alegación de datos o circunstancias falsos o la omisión de comunicaciones obligatorias dentro de los plazos establecidos, siempre que no constituya infracción penal.

10. El incumplimiento de la obligación de obtener la documentación personal legalmente exigida, así como la omisión negligente de la denuncia de su sustracción o extravío.

11. La negligencia en la custodia y conservación de la documentación personal legalmente exigida, considerándose como tal la tercera y posteriores pérdidas o extravíos en el plazo de un año.

12. La negativa a entregar la documentación personal legalmente exigida cuando se hubiese acordado su retirada o retención.

13. Los daños o el deslucimiento de bienes muebles o inmuebles de uso o servicio público, así como de bienes muebles o inmuebles privados en la vía pública, cuando no constituyan infracción penal.

14. El escalamiento de edificios o monumentos sin autorización cuando exista un riesgo cierto de que se ocasionen daños a las personas o a los bienes.

15. La remoción de vallas, encintados u otros elementos fijos o móviles colocados por las Fuerzas y Cuerpos de Seguridad para delimitar perímetros de seguridad, aun con carácter preventivo, cuando no constituya infracción grave.

16. Dejar sueltos o en condiciones de causar daños animales feroces o dañinos, así como abandonar animales domésticos en condiciones en que pueda peligrar su vida.

17. El consumo de bebidas alcohólicas en lugares, vías, establecimientos o transportes públicos cuando perturbe gravemente la tranquilidad ciudadana.

Artículo 38. *Prescripción de las infracciones.*

1. Las infracciones administrativas tipificadas en esta Ley prescribirán a los seis meses, al año o a los dos años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

2. Los plazos señalados en esta Ley se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas y de infracciones de efectos permanentes, los plazos se computarán, respectivamente, desde el día en que se realizó la última infracción y desde que se eliminó la situación ilícita.

3. La prescripción se interrumpirá por cualquier actuación administrativa de la que tenga conocimiento formal el interesado dirigida a la sanción de la infracción, reanudándose el cómputo del plazo de prescripción si el procedimiento estuviera paralizado más de un mes por causa no imputable al presunto responsable.

4. Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización en los términos del apartado 2 del artículo 45.

Artículo 39. *Sanciones.*

1. Las infracciones muy graves se sancionarán con multa de 30.001 a 600.000 euros; las graves, con multa de 601 a 30.000 euros, y las leves, con multa de 100 a 600 euros.

De acuerdo con lo dispuesto en el artículo 33.2, los tramos correspondientes a los grados máximo, medio y mínimo de las multas previstas por la comisión de infracciones graves y muy graves serán los siguientes:

a) Para las infracciones muy graves, el grado mínimo comprenderá la multa de 30.001 a 220.000 euros; el grado medio, de 220.001 a 410.000 euros, y el grado máximo, de 410.001 a 600.000 euros.

b) Para las infracciones graves, el grado mínimo comprenderá la multa de 601 a 10.400; el grado medio, de 10.401 a 20.200 euros, y el grado máximo, de 20.201 a 30.000 euros.

2. La multa podrá llevar aparejada alguna o algunas de las siguientes sanciones accesorias, atendiendo a la naturaleza de los hechos constitutivos de la infracción:

a) La retirada de las armas y de las licencias o permisos correspondientes a las mismas.

b) El comiso de los bienes, medios o instrumentos con los que se haya preparado o ejecutado la infracción y, en su caso, de los efectos procedentes de ésta, salvo que unos u otros pertenezcan a un tercero de buena fe no responsable de dicha infracción que los haya adquirido legalmente. Cuando los instrumentos o efectos sean de lícito comercio y su valor no guarde relación con la naturaleza o gravedad de la infracción, el órgano competente para imponer la sanción que proceda podrá no acordar el comiso o acordarlo parcialmente.

c) La suspensión temporal de las licencias, autorizaciones o permisos desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses para las infracciones graves, en el ámbito de las materias reguladas en el capítulo IV de esta Ley. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

d) La clausura de las fábricas, locales o establecimientos, desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses por infracciones graves, en el ámbito de las materias reguladas en el capítulo IV de esta Ley. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

Artículo 40. *Prescripción de las sanciones.*

1. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

2. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquél se paraliza durante más de un mes por causa no imputable al infractor.

Artículo 41. *Habilitación reglamentaria.*

Las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones tipificadas en esta Ley que, sin constituir nuevas infracciones o sanciones, ni alterar su naturaleza y límites, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las sanciones correspondientes.

Artículo 42. *Reparación del daño e indemnización.*

1. Si las conductas sancionadas hubieran ocasionado daños o perjuicios a la administración pública, la resolución del procedimiento contendrá un pronunciamiento expreso acerca de los siguientes extremos:

a) La exigencia al infractor de la reposición a su estado originario de la situación alterada por la infracción.

b) Cuando ello no fuera posible, la indemnización por los daños y perjuicios causados, si éstos hubiesen quedado determinados durante el procedimiento. Si el importe de los daños y perjuicios no hubiese quedado establecido, se determinará en un procedimiento complementario, susceptible de terminación convencional, cuya resolución pondrá fin a la vía administrativa.

2. La responsabilidad civil derivada de una infracción será siempre solidaria entre todos los causantes del daño.

3. Cuando sea declarado autor de los hechos cometidos un menor de dieciocho años no emancipado o una persona con la capacidad modificada judicialmente, responderán, solidariamente con él, de los daños y perjuicios ocasionados sus padres, tutores, curadores, acogedores o guardadores legales o de hecho, según proceda.

Artículo 43. *Registro Central de Infracciones contra la Seguridad Ciudadana.*

1. A efectos exclusivamente de apreciar la reincidencia en la comisión de infracciones tipificadas en esta Ley, se crea en el Ministerio del Interior un Registro Central de Infracciones contra la Seguridad Ciudadana.

Las comunidades autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio, podrán crear sus propios registros de infracciones contra la seguridad ciudadana.

2. Reglamentariamente se regulará la organización y funcionamiento del Registro Central de Infracciones contra la Seguridad Ciudadana, en el que únicamente se practicarán los siguientes asientos:

a) Datos personales del infractor.

b) Infracción cometida.

c) Sanción o sanciones firmes en vía administrativa impuestas, con indicación de su alcance temporal, cuando proceda.

d) Lugar y fecha de la comisión de la infracción.

e) Órgano que haya impuesto la sanción.

3. Las personas a las que se haya impuesto una sanción que haya adquirido firmeza en vía administrativa serán informadas de que se procederá a la práctica de los correspondientes asientos en el Registro Central de Infracciones contra la Seguridad Ciudadana. Podrán solicitar el acceso, cancelación o rectificación de sus datos de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo. Los asientos se cancelarán de oficio transcurridos tres años cuando se trate de infracciones muy graves, dos años en el caso de infracciones graves y uno en el de infracciones leves, a contar desde la firmeza de la sanción.

4. Las autoridades y órganos de las distintas administraciones públicas con competencia sancionadora en materia de seguridad ciudadana, de acuerdo con esta Ley, comunicarán al Registro Central de Infracciones contra la Seguridad Ciudadana las resoluciones sancionadoras dictadas, una vez firmes en vía administrativa. Asimismo, a estos efectos, dichas administraciones públicas tendrán acceso a los datos obrantes en ese Registro Central.

Sección 3.ª Procedimiento sancionador

Artículo 44. *Régimen jurídico.*

El ejercicio de la potestad sancionadora en materia de protección de la seguridad ciudadana se regirá por el título IX de la Ley 30/1992, de 26 de noviembre, y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este capítulo.

Artículo 45. *Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.*

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

Artículo 46. *Acceso a los datos de otras administraciones públicas.*

1. Las autoridades y órganos de las distintas administraciones públicas competentes para imponer sanciones de acuerdo con esta Ley podrán acceder a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, sin necesidad de consentimiento previo del titular de los datos, con las garantías de seguridad, integridad y disponibilidad, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre.

2. A los exclusivos efectos de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria y la Tesorería General de la Seguridad Social, en los términos establecidos en la normativa tributaria o de la seguridad social, así como el Instituto Nacional de Estadística, en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquéllos el acceso a los ficheros en los que obren datos que hayan de constar en dichos procedimientos, sin que sea preciso el consentimiento de los interesados.

Artículo 47. *Medidas provisionales anteriores al procedimiento.*

1. Los agentes de la autoridad intervendrán y aprehenderán cautelarmente los instrumentos utilizados para la comisión de la infracción, así como el dinero, los frutos o los productos directamente obtenidos, que se mantendrán en los depósitos establecidos al efecto o bajo la custodia de las Fuerzas y Cuerpos de Seguridad mientras se tramita el procedimiento sancionador o hasta que, en su caso, se resuelva la devolución o se decrete el comiso.

Sin perjuicio de lo previsto en el apartado 3 del artículo 49, si la aprehensión fuera de bienes fungibles y el coste del depósito superase el valor venal, éstos se destruirán o se les dará el destino adecuado, de acuerdo con el procedimiento que se establezca reglamentariamente.

2. Excepcionalmente, en los supuestos de grave riesgo o peligro inminente para personas o bienes, las medidas provisionales previstas en el apartado 1 del artículo 49, salvo la del párrafo f), podrán ser adoptadas directamente por los agentes de la autoridad con carácter previo a la iniciación del procedimiento, debiendo ser ratificadas, modificadas o revocadas en el acuerdo de incoación en el plazo máximo de quince días. En todo caso, estas medidas quedarán sin efecto si, transcurrido dicho plazo, no se incoa el procedimiento o el acuerdo de incoación no contiene un pronunciamiento expreso acerca de las mismas.

Artículo 48. *Actuaciones previas.*

1. Con anterioridad a la incoación del procedimiento se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que las justifiquen. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

Las actuaciones previas se incorporarán al procedimiento sancionador.

2. Las actuaciones previas podrán desarrollarse sin intervención del presunto responsable, si fuera indispensable para garantizar el buen fin de la investigación, dejando constancia escrita en las diligencias instruidas al efecto de las razones que justifican su no intervención.

3. La práctica de actuaciones previas no interrumpirá la prescripción de las infracciones.

Artículo 49. *Medidas de carácter provisional.*

1. Incoado el expediente, el órgano competente para resolver podrá adoptar en cualquier momento, mediante acuerdo motivado, las medidas de carácter provisional que resulten necesarias para asegurar la eficacia de la resolución que pudiera recaer, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción o preservar la seguridad ciudadana, sin que en ningún caso puedan tener carácter sancionador. Dichas medidas serán proporcionadas a la naturaleza y gravedad de la infracción y podrán consistir especialmente en:

a) El depósito en lugar seguro de los instrumentos o efectos utilizados para la comisión de las infracciones y, en particular, de las armas, explosivos, aerosoles, objetos o materias potencialmente peligrosos para la tranquilidad ciudadana, drogas tóxicas, estupefacientes o sustancias psicotrópicas.

b) La adopción de medidas de seguridad de las personas, bienes, establecimientos o instalaciones que se encuentren en situación de peligro, a cargo de sus titulares.

c) La suspensión o clausura preventiva de fábricas, locales o establecimientos susceptibles de afectar a la seguridad ciudadana.

d) La suspensión parcial o total de las actividades en los establecimientos que sean notoriamente vulnerables y no tengan en funcionamiento las medidas de seguridad necesarias.

e) La adopción de medidas de seguridad de las personas y los bienes en infraestructuras e instalaciones en las que se presten servicios básicos para la comunidad.

f) La suspensión de la actividad objeto de autorizaciones, permisos, licencias y otros documentos expedidos por las autoridades administrativas, en el marco de la normativa que le sea de aplicación.

g) La suspensión en la venta, reventa o venta ambulante de las entradas del espectáculo o actividad recreativa cuya celebración o desarrollo pudiera implicar un riesgo para la seguridad ciudadana.

2. Los gastos ocasionados por la adopción de las medidas provisionales correrán a cargo del causante de los hechos objeto del expediente sancionador.

3. La duración de las medidas de carácter provisional no podrá exceder de la mitad del plazo previsto en esta Ley para la sanción que pudiera corresponder a la infracción cometida, salvo acuerdo debidamente motivado adoptado por el órgano competente.

4. El acuerdo de adopción de medidas provisionales se notificará a los interesados en el domicilio del que tenga constancia por cualquier medio la administración o, en su caso, por

medios electrónicos, con indicación de los recursos procedentes contra el mismo, órgano ante el que deban presentarse y plazos para interponerlos. La autoridad competente para su adopción podrá acordar que sea objeto de conocimiento general cuando ello sea necesario para garantizar la seguridad ciudadana, con sujeción a lo dispuesto en la legislación en materia de protección de datos de carácter personal.

5. Las medidas adoptadas serán inmediatamente ejecutivas, sin perjuicio de que los interesados puedan solicitar su suspensión justificando la apariencia de buen derecho y la existencia de daños de difícil o imposible reparación, prestando, en su caso, caución suficiente para asegurar el perjuicio que se pudiera derivar para la seguridad ciudadana.

6. Las medidas provisionales acordadas podrán ser modificadas o levantadas cuando varíen las circunstancias que motivaron su adopción y, en todo caso, se extinguirán con la resolución que ponga fin al procedimiento.

Artículo 50. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurrido un año desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Artículo 51. *Efectos de la resolución.*

En el ámbito de la Administración General del Estado, la resolución del procedimiento sancionador será recurrible de conformidad con la Ley 30/1992, de 26 de noviembre. Contra la resolución que ponga fin a la vía administrativa podrá interponerse recurso contencioso-administrativo, en su caso, por el procedimiento para la protección de los derechos fundamentales de la persona, en los términos de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Artículo 52. *Valor probatorio de las declaraciones de los agentes de la autoridad.*

En los procedimientos sancionadores que se instruyan en las materias objeto de esta Ley, las denuncias, atestados o actas formulados por los agentes de la autoridad en ejercicio de sus funciones que hubiesen presenciado los hechos, previa ratificación en el caso de haber sido negados por los denunciados, constituirán base suficiente para adoptar la resolución que proceda, salvo prueba en contrario y sin perjuicio de que aquéllos deban aportar al expediente todos los elementos probatorios disponibles.

Artículo 53. *Ejecución de la sanción.*

1. Una vez firme en vía administrativa, se procederá a la ejecución de la sanción conforme a lo previsto en esta Ley.

2. El cumplimiento de la sanción de suspensión de las licencias, autorizaciones o permisos se iniciará transcurrido un mes desde que la sanción haya adquirido firmeza en vía administrativa.

3. Las sanciones pecuniarias que no hayan sido abonadas previamente deberán hacerse efectivas dentro de los quince días siguientes a la fecha de la firmeza de la sanción. Una vez vencido el plazo de ingreso sin que se hubiese satisfecho la sanción, su exacción se llevará a cabo por el procedimiento de apremio. A tal efecto, será título ejecutivo la providencia de apremio notificada al deudor, expedida por el órgano competente de la administración.

4. Cuando las sanciones hayan sido impuestas por la Administración General del Estado, los órganos y procedimientos de la recaudación ejecutiva serán los establecidos en el Reglamento General de Recaudación, aprobado por el Real Decreto 939/2005, de 29 de julio.

5. En caso de que la resolución acuerde la devolución de los instrumentos aprehendidos cautelarmente a los que se refiere el apartado 1 del artículo 47, transcurrido un mes desde la notificación de la misma sin que el titular haya recuperado el objeto aprehendido, se procederá a su destrucción o se le dará el destino adecuado en el marco de esta Ley.

Artículo 54. *Procedimiento abreviado.*

1. Una vez notificado el acuerdo de incoación del procedimiento para la sanción de infracciones graves o leves, el interesado dispondrá de un plazo de quince días para realizar el pago voluntario con reducción de la sanción de multa, o para formular las alegaciones y proponer o aportar las pruebas que estime oportunas.

Si efectúa el pago de la multa en las condiciones indicadas en el párrafo anterior, se seguirá el procedimiento sancionador abreviado, y, en caso de no hacerlo, el procedimiento sancionador ordinario.

2. El procedimiento sancionador abreviado no será de aplicación a las infracciones muy graves.

3. Una vez realizado el pago voluntario de la multa dentro del plazo de quince días contados desde el día siguiente al de su notificación, se tendrá por concluido el procedimiento sancionador con las siguientes consecuencias:

a) La reducción del 50 por ciento del importe de la sanción de multa.

b) La renuncia a formular alegaciones. En el caso de que fuesen formuladas se tendrán por no presentadas.

c) La terminación del procedimiento, sin necesidad de dictar resolución expresa, el día en que se realice el pago, siendo recurrible la sanción únicamente ante el orden jurisdiccional contencioso-administrativo.

Disposición adicional primera. *Régimen de control de precursores de drogas y explosivos.*

El sistema de otorgamiento de licencias de actividad, así como el régimen sancionador aplicable en caso de infracción de las disposiciones comunitarias e internacionales para la vigilancia del comercio de precursores de drogas y explosivos se regirá por lo dispuesto en sus legislaciones específicas.

Disposición adicional segunda. *Régimen de protección de las infraestructuras críticas.*

La protección de las infraestructuras críticas se regirá por su normativa específica y supletoriamente por esta Ley.

Disposición adicional tercera. *Comparecencia obligatoria en los procedimientos para la obtención del Documento Nacional de Identidad y el pasaporte.*

En los procedimientos administrativos de obtención del Documento Nacional de Identidad y el pasaporte será obligatoria la comparecencia del interesado ante los órganos o unidades administrativas competentes para su tramitación.

Excepcionalmente podrá eximirse de la comparecencia personal al solicitante de un pasaporte provisional en una Misión diplomática u Oficina consular española por razones justificadas de enfermedad, riesgo, lejanía u otras análogas y debidamente acreditadas que impidan o dificulten gravemente la comparecencia.

Disposición adicional cuarta. *Comunicaciones del Registro Civil.*

A efectos de dar cumplimiento a lo dispuesto en el artículo 8.3 de la Ley, el Registro Civil comunicará al Ministerio del Interior las inscripciones de resoluciones de capacidad modificada judicialmente, los fallecimientos o las declaraciones de ausencia o fallecimiento, de acuerdo con lo dispuesto en el artículo 80 de la Ley 20/2011, de 21 de julio, del Registro Civil.

Disposición adicional quinta. *Suspensión de sanciones pecuniarias impuestas por infracciones en materia de consumo de drogas tóxicas, estupefacientes o sustancias psicotrópicas cometidas por menores de edad.*

Las multas que se impongan a los menores de edad por la comisión de infracciones en materia de consumo o tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas podrán suspenderse siempre que, a solicitud de los infractores y sus representantes legales, aquéllos accedan a someterse a tratamiento o rehabilitación, si lo precisan, o a actividades de reeducación. En caso de que los infractores abandonen el tratamiento o rehabilitación o las actividades reeducativas, se procederá a ejecutar la sanción económica.

Reglamentariamente se regularán los términos y condiciones de la remisión parcial de sanciones prevista en esta disposición adicional.

Disposición adicional sexta. *Infraestructuras e instalaciones en las que se prestan servicios básicos para la comunidad.*

A los efectos de lo dispuesto en los artículos 35.1 y 36.9, se entenderá por infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad:

a) Centrales nucleares, petroquímicas, refinerías y depósitos de combustible.
b) Puertos, aeropuertos y demás infraestructuras de transporte.
c) Servicios de suministro y distribución de agua, gas y electricidad.
d) Infraestructuras de telecomunicaciones.

Disposición adicional séptima. *No incremento de gasto público.*

Las medidas contempladas en esta Ley no generarán incremento de dotaciones ni de retribuciones, ni de otros gastos de personal al servicio del sector público.

Disposición transitoria única. *Procedimientos sancionadores iniciados a la entrada en vigor de esta Ley.*

Los procedimientos sancionadores iniciados a la entrada en vigor de esta Ley se regirán por la legislación anterior, salvo que esta Ley contenga disposiciones más favorables para el interesado.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.
2. Asimismo, quedan derogadas cuantas disposiciones, de igual o inferior rango, se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Régimen especial de Ceuta y Melilla.*

1. Se adiciona una disposición adicional décima a la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, con la siguiente redacción:

> **«Disposición adicional décima.** *Régimen especial de Ceuta y Melilla.*
>
> 1. Los extranjeros que sean detectados en la línea fronteriza de la demarcación territorial de Ceuta o Melilla mientras intentan superar los elementos de contención fronterizos para cruzar irregularmente la frontera podrán ser rechazados a fin de impedir su entrada ilegal en España.
> 2. En todo caso, el rechazo se realizará respetando la normativa internacional de derechos humanos y de protección internacional de la que España es parte.
> 3. Las solicitudes de protección internacional se formalizarán en los lugares habilitados al efecto en los pasos fronterizos y se tramitarán conforme a lo establecido en la normativa en materia de protección internacional.»

2. La disposición final cuarta de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, queda redactada del siguiente modo:

> **«Disposición final cuarta.** *Preceptos no orgánicos.*
>
> 1. Tienen naturaleza orgánica los preceptos contenidos en los siguientes artículos de esta Ley: 1, 2, 3, 4.1, 4.3, 5, 6, 7, 8, 9, 11, 15, 16, 17, 18, 18 bis, 19, 20, 21, 22.1, 23, 24, 25, 25 bis, 27, 29, 30, 30 bis, 31, 31 bis, 33, 34, 36, 37, 39, 40, 41, 42, 53, 54, 55, 57, 58, 59, 59 bis, 60, 61, 62, 62 bis, 62 ter, 62 quáter, 62 quinquies, 62 sexies, 63, 63 bis, 64, 66, 71, las disposiciones adicionales tercera a octava y décima y las disposiciones finales.
>
> 2. Los preceptos no incluidos en el apartado anterior no tienen naturaleza orgánica.»

Disposición final segunda. *Títulos competenciales.*

Las disposiciones de esta Ley se dictan al amparo del artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, excepto los artículos 28 y 29, que se dictan al amparo del artículo 149.1.26.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de régimen de producción, comercio, tenencia y uso de armas y explosivos.

Disposición final tercera. *Preceptos que tienen carácter de Ley orgánica.*

1. Tienen carácter orgánico los preceptos de esta Ley que se relacionan a continuación:

El capítulo I, excepto el artículo 5.
Los artículos 9 y 11 del capítulo II.
El capítulo III.
Del capítulo V, el apartado 3 del artículo 30; el ordinal 1 del artículo 35; los ordinales 2, 7, 8 y 23 del artículo 36, y los ordinales 1 y 4 del artículo 37.
La disposición derogatoria única.
La disposición final primera.
La disposición final tercera.

2. Los preceptos no incluidos en el apartado anterior no tienen carácter orgánico.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno, en el ámbito de sus competencias, para dictar las disposiciones necesarias para el desarrollo y aplicación de lo establecido en esta Ley.

Disposición final quinta. *Entrada en vigor.*

Esta Ley orgánica entrará en vigor el 1 de julio de 2015, salvo la disposición final primera, que entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 19

Ley 5/2014, de 4 de abril, de Seguridad Privada

Jefatura del Estado
«BOE» núm. 83, de 5 de abril de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-3649

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La seguridad no es solo un valor jurídico, normativo o político; es igualmente un valor social. Es uno de los pilares primordiales de la sociedad, se encuentra en la base de la libertad y la igualdad y contribuye al desarrollo pleno de los individuos.

Los Estados, al establecer el modelo legal de seguridad privada, lo perfilan como la forma en la que los agentes privados contribuyen a la minoración de posibles riesgos asociados a su actividad industrial o mercantil, obtienen seguridad adicional más allá de la que provee la seguridad pública o satisfacen sus necesidades de información profesional con la investigación de asuntos de su legítimo interés. En esta óptica, la existencia de la seguridad privada se configura como una medida de anticipación y prevención frente a posibles riesgos, peligros o delitos. La consideración de la seguridad privada como una actividad con entidad propia, pero a la vez como parte integrante de la seguridad pública, es hoy un hecho innegable.

No solo en España sino fundamentalmente en nuestro entorno europeo, la seguridad privada se ha convertido en un verdadero actor de las políticas globales y nacionales de seguridad.

En los últimos años se han producido notables avances en la consideración ciudadana y en el replanteamiento del papel del sector privado de la seguridad, reconociéndose la importancia, eficacia y eficiencia de las alianzas público-privadas como medio para hacer frente y resolver los problemas acuciantes y variados de seguridad que se producen en la sociedad. Cada vez más, la seguridad privada se considera una parte indispensable del conjunto de medidas destinadas a la protección de la sociedad y a la defensa de los derechos y legítimos intereses de los ciudadanos.

La seguridad, entendida como pilar básico de la convivencia ejercida en régimen de monopolio por el poder público del Estado, tanto en su vertiente preventiva como investigadora, encuentra en la realización de actividades de seguridad por otras instancias sociales o agentes privados una oportunidad para verse reforzada, y una forma de articular el reconocimiento de la facultad que tienen los ciudadanos de crear o utilizar los servicios privados de seguridad con las razones profundas sobre las que se asienta el servicio público de la seguridad.

La proyección de la Administración del Estado sobre la prestación de servicios de seguridad por entidades privadas y sobre su personal se basa en el hecho de que los servicios que prestan forman parte del núcleo esencial de la competencia exclusiva en materia de seguridad pública atribuida al Estado por el artículo 149.1.29.ª de la Constitución, y en la misión que, según el artículo 104 del propio texto fundamental, incumbe a las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

A partir de ahí, se establece un conjunto de controles e intervenciones administrativas que condicionan el ejercicio de las actividades de seguridad por los particulares. Ello significa que las Fuerzas y Cuerpos de Seguridad han de estar permanentemente presentes en el desarrollo de las actividades privadas de seguridad, conociendo la información trascendente para la seguridad pública que en las mismas se genera y actuando con protagonismo indiscutible, siempre que tales actividades detecten el acaecimiento de hechos delictivos o que puedan afectar a la seguridad ciudadana.

La defensa de la seguridad y el legítimo derecho a usarla no pueden ser ocasión de agresión o desconocimiento de derechos o invasión de las esferas jurídicas y patrimoniales de otras personas. Y ésta es una de las razones que justifican la intensa intervención en la organización y desarrollo de las actividades de las entidades privadas de seguridad y de su personal, por parte de la Fuerzas y Cuerpos de Seguridad, que tienen la misión constitucional de proteger los derechos fundamentales de todos los ciudadanos y garantizar su seguridad.

Desde otra perspectiva, pero igualmente integrada en el objeto de regulación de esta ley, es necesario dar el paso de reconocer la especificidad de los servicios de investigación privada el papel que han alcanzado en nuestra sociedad en los últimos años. Siendo diferentes de los demás servicios de seguridad privada, su acogida en esta norma, dentro del conjunto de actividades de seguridad privada, refleja la configuración de aquéllos como un elemento más que contribuye a garantizar la seguridad de los ciudadanos, entendida en un sentido amplio.

II

La Ley 23/1992, de 30 de julio, de Seguridad Privada, que ahora se deroga, vino a ordenar un sector hasta entonces regulado por una normativa dispersa, de rango inferior y de orientación preconstitucional en algunos casos, que contemplaba una realidad todavía incipiente, y a la que dicho marco legal permitió desarrollarse de forma armónica hasta alcanzar la importancia y transcendencia que ahora tiene, habiendo sabido concitar la generalizada aceptación de la sociedad española.

Ciertamente, la Ley 23/1992, de 30 de julio, así como su normativa de desarrollo, ha supuesto un gran avance para la evolución de la seguridad privada en España, e incluso ha constituido un modelo para procesos normativos análogos en otros Estados de la Unión Europea. Sin embargo, resulta imprescindible alumbrar una nueva normativa legal que dé solución a los problemas detectados y permita seguir evolucionando a un sector de la industria de servicios española que tanto ha contribuido a la seguridad.

En efecto, la regulación del año 1992 resulta hoy claramente insuficiente, lo que se percibe en sus profundas lagunas y carencias, paliadas parcialmente en el posterior reglamento de desarrollo, aprobado por el Real Decreto 2364/1994, de 9 de diciembre, e incluso por normas de rango inferior o simples resoluciones. Han sido en muchas ocasiones este tipo de normas las que han permitido que la Ley 23/1992, de 30 de julio, haya podido mantener su vigencia hasta el momento actual.

Además, la pertenencia de nuestro país a la Unión Europea ha obligado a que la norma fundamental que regula en España la seguridad privada, la Ley 23/1992, de 30 de junio,

haya debido ser modificada por los Reales Decretos-leyes 2/1999, de 29 de enero, y 8/2007, de 14 de septiembre, así como por la Ley 25/2009, de 22 de diciembre, de modificación de diversas Leyes para su adaptación a la Ley sobre libre acceso a las actividades de servicios y su ejercicio, con la finalidad de adaptarse cada vez a un entorno más abierto y globalizado, fenómeno que la citada ley, lógicamente, consideró de manera muy colateral.

Otros dos factores determinantes de la necesidad de sustituir la vigente ley cabecera de este sector del ordenamiento jurídico son los importantísimos cambios tecnológicos, que condicionan la prestación de servicios de seguridad, y la tendencia a la integración de las distintas seguridades en un concepto de seguridad integral, cuestión a tener en cuenta tanto en el ámbito de las actividades como en el de las funciones y servicios que presta el personal de seguridad privada, aspectos éstos que la Ley 23/1992, de 30 de julio, no podía contemplar.

Pasados veinte años desde su promulgación, ante un sector maduro y completamente profesionalizado, con presencia en todos los lugares y niveles de la vida del país y de sus ciudadanos, y ante una realidad completamente diferente a la del año 1992, es necesario aprobar una nueva norma que permita solucionar los problemas de funcionamiento detectados a lo largo de estas dos décadas pasadas.

Este fenómeno de insuficiencia de regulación se da aún más, si cabe, con las actividades de investigación privada y los detectives privados, cuya inserción tangencial en la Ley 23/1992, de 30 de julio, vino a abundar en el problema expuesto. En efecto son muy escasas las prevenciones sobre dichas actividades y personal no sólo en sede legal, sino también reglamentaria, por lo cual esta ley afronta de manera decidida y completa, en lo que le corresponde, la definición de su contenido, perfiles, limitaciones y características de quienes, convenientemente formados y habilitados, la desarrollan. De esta manera la regulación de las actividades y el personal de investigación privada pasa a constituir uno de los elementos fundamentales de la nueva ley, abandonando la presencia colateral que tiene en la vigente normativa.

III

Al contrario de la anterior regulación, la nueva ley representa un tratamiento total y sistemático de la seguridad privada en su conjunto, que pretende abarcar toda la realidad del sector existente en España, al tiempo que lo prepara para el futuro.

En consecuencia, es preciso transitar desde la concepción de control y sanción, que inspira el preámbulo y el articulado de la Ley 23/1992, de 30 de julio, y que tuvo su razón de ser en aquel momento, hasta una norma que permita aprovechar las enormes potencialidades que presenta la seguridad privada desde la perspectiva del interés público.

Es por eso que la nueva regulación contempla, entre otros objetivos, la mejora de la eficacia en la prestación de los servicios de seguridad privada en lo relativo a organización y planificación, formación y motivación del personal de seguridad; la eliminación de las situaciones que dan lugar al intrusismo tanto de las empresas como del personal; la dotación al personal de seguridad privada del respaldo jurídico necesario para el ejercicio de sus funciones legales, y los elementos de colaboración entre la seguridad privada y la seguridad pública.

La ley pasa de poner el acento en el principio de la subordinación a desarrollar más eficazmente el principio de complementariedad a través de otros que lo desarrollan, como los de cooperación o de corresponsabilidad, mediante una técnica legislativa más flexible que permite una adaptación permanente a los cambios que experimente la sociedad sin que sea precisa una reforma de rango legal para ello.

En la relación especial que mantiene la seguridad privada con las Fuerzas y Cuerpos de Seguridad, auténticos garantes del sistema de libertades y derechos que constitucionalmente protegen, se hace necesario avanzar en fórmulas jurídicas que reconozcan el papel auxiliar y especialmente colaborador desempeñado por la seguridad privada, de forma que, además de integrar funcionalmente sus capacidades en el sistema público de seguridad, les haga partícipes de la información que resulte necesaria para el mejor cumplimiento de sus deberes.

Se aborda, así, una reforma en profundidad de la regulación legal hasta ahora vigente que pivota sobre dos ejes. En primer lugar, sobre la base irrenunciable de la preeminencia

de la seguridad pública sobre la seguridad privada, se realiza una adecuación de la normativa que permita su adaptación y dé respuesta a la necesidad real de seguridad en cada momento, de manera que se aprovechen todas sus potencialidades. En segundo lugar, los poderes de intervención y control público sobre la seguridad privada se focalizan en los aspectos verdaderamente esenciales para la seguridad pública, desregulando los aspectos accesorios que no tienen una directa relación con el servicio de seguridad, al tiempo que se moderniza su gestión y se potencia su colaboración con la seguridad pública.

En resumen, puede decirse que el conjunto de los cambios propuestos en la nueva ley, además de mejorar y resolver problemas técnicos, de gestión y operativos, profundiza decididamente en el actual modelo español de seguridad privada (complementaria, subordinada, colaboradora y controlada por la seguridad pública), apostando por su papel preventivo en beneficio de la seguridad general, y lo hace aprovechando e integrando funcionalmente todo su potencial informativo, de recursos humanos y de medios materiales, al servicio de la protección y seguridad del conjunto de la ciudadanía, de forma compatible con el legítimo interés que persiguen las entidades privadas de seguridad.

Este mismo enfoque inspira los preceptos que se dedican a la investigación privada. En este punto, el legislador, como en las restantes actividades contempladas en la ley, tiene que hacer compatible ese enfoque positivo con una serie de prevenciones indispensables para garantizar los derechos de los ciudadanos, especialmente los del artículo 18 de la Constitución.

IV

Uno de los aspectos donde más se ha puesto de manifiesto el cambio habido desde la aprobación de la Ley 23/1992, de 30 de julio, es en la participación de las comunidades autónomas en la materia. Lo que entonces era algo residual se ha transformado en un fenómeno de mayor calado, pues a las comunidades autónomas con competencia estatutariamente asumida para la protección de personas y bienes y el mantenimiento del orden público, se van uniendo otras comunidades autónomas cuyos nuevos estatutos de autonomía reconocen su competencia sobre la seguridad privada, aunque en ambos casos con sujeción a lo que el Estado regule de acuerdo con el artículo 149.1.29.ª de la Constitución.

Así, la nueva ley quiere reconocer este cambio de situación y contemplar el fenómeno de una manera global, no tangencial, como hasta el momento, reflejando los diferentes niveles competenciales en función de las previsiones estatutarias.

Para que la actuación de las distintas administraciones públicas sea coherente con el mantenimiento de la armonía del sistema, es fundamental incidir en los principios de coordinación y cooperación interadministrativa.

Al objeto de evitar interferencias y duplicidades, se prevén mecanismos de coordinación institucional, se clarifica el reparto de competencias estatales y autonómicas, se afianza la competencia exclusiva del Estado en materia normativa y se sitúan en la órbita ejecutiva las competencias de las comunidades autónomas.

V

Se pasa de un tratamiento normativo parcial a una ley generalista, reguladora de la totalidad de materias que configuran el sector de la seguridad privada, dotada de sistematicidad normativa a lo largo de sus siete títulos, con un desglose de materias que abarcan desde lo más general hasta lo más específico.

Así, en el título preliminar se ha aprovechado para dar definición legal a conceptos o términos que hasta ahora permanecían jurídicamente imprecisos o indeterminados, tales como el propio de seguridad privada, o los de actividades de seguridad, servicios de seguridad, funciones de seguridad, medidas de seguridad, despachos de detectives privados u otros de significada importancia, lo que sin duda alguna ha de tener una directa repercusión favorable en la mejora de la seguridad jurídica.

En esta línea, por primera vez se fija el ámbito material y la finalidad a la que sirve la propia seguridad privada, que no puede ser otra que contribuir, con su acción profesional, a completar la seguridad pública de la que forma parte.

Otras importantes novedades que la nueva ley incorpora en su título preliminar son las referidas a la actualización del ámbito de las actividades de seguridad privada; se regulan las llamadas actividades compatibles, consistentes en todas aquellas materias que rodean o tienen incidencia directa con el mundo de la seguridad, y, por otra parte, se completan y perfilan mejor las actividades de seguridad privada, como es el caso de la investigación privada, que se incluye con normalidad en el catálogo de actividades de seguridad.

Además, se reconoce a los operadores de seguridad la condición de personal acreditado como respuesta al gran avance tecnológico y profunda transformación que ha experimentado la actividad de verificación de alarmas.

La seguridad de la información y las comunicaciones aparece por primera vez configurada no como actividad específica de seguridad privada, sino como actividad compatible que podrá ser desarrollada tanto por empresas de seguridad como por las que no lo sean, y que, por su incidencia directa en la seguridad de las entidades públicas y privadas, llevará implícito el sometimiento a ciertas obligaciones por parte de proveedores y usuarios.

Igualmente, en la línea de reducir restricciones a la libre competencia, se liberaliza la actividad de planificación, consultoría y asesoramiento en materia de seguridad privada, que pasa a considerarse como una actividad compatible no reservada a las empresas de seguridad privada, ya que su afección a esta última, y mediatamente a la seguridad pública, no es directa.

También se ha aprovechado para realizar una necesaria matización del principio general de exclusión de la seguridad privada de los espacios públicos, cuya formulación actual, excesivamente rígida, ha dificultado o impedido la necesaria autorización de servicios en beneficio del ciudadano, que resulta hoy obsoleta.

En el título I se plasma una de las ideas claves que han inspirado la redacción de la ley, como es la coordinación y la colaboración entre los servicios de seguridad privada y las Fuerzas y Cuerpos de Seguridad, con el único objetivo de mejorar la seguridad pública, mediante el intercambio de información siempre con todas las garantías legales, y la apuesta decidida por unos órganos de encuentro que han de ser mucho más proactivos que hasta el momento.

En el título II se da rango legal a algunos preceptos dedicados a la regulación de empresas de seguridad y despachos de detectives, o a los registros de ambos, que se unifican en el nuevo Registro Nacional de Seguridad Privada.

Además, se regula un sistema flexible que permitirá, cuando sea necesario por razón de las instalaciones vigiladas, aumentar los requisitos de las empresas, o reducirlos por razón de la actividad desempeñada.

En línea con el favorecimiento de la actividad económica, la ley sustituye el sistema más gravoso de la autorización administrativa por el de la declaración responsable para los centros de formación de personal de seguridad privada, los despachos de detectives privados y las empresas de instalación y mantenimiento.

En el título III se regulan cuestiones anteriormente dejadas al reglamento, donde no tenían correcta ubicación, tales como las relativas a las funciones de gran parte del personal de seguridad, ya que la Ley 23/1992, de 30 de julio, tan sólo se ocupaba de las funciones de los vigilantes de seguridad y de los detectives privados.

La ley modifica el nombre de los guardas particulares del campo, para configurarlos, más adecuadamente, como guardas rurales.

Por otra parte, se resuelve el problema del requisito de la nacionalidad española o de un Estado de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para poder acceder a las profesiones de seguridad, que ahora se amplía a los nacionales de terceros Estados que tengan suscrito con España un convenio internacional en el que se contemple tal posibilidad a los nacionales de ambos Estados.

Otra de las novedades que se incorpora en materia de personal, largamente demandada por el sector, es la protección jurídica análoga a la de los agentes de la autoridad del personal de seguridad privada frente a las agresiones o desobediencias de que pueden ser objeto cuando desarrollen, debidamente identificados, las actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad.

Además de eliminar el inadecuado y distorsionador período de inactividad, que tantas dificultades y problemas ha supuesto para la normal reincorporación al sector del personal

de seguridad privada, en la formación del personal, junto al actual sistema de acceso a la profesión a través exclusivamente del Ministerio del Interior, se da cabida a otras posibilidades de acceso mediante el sistema que determine el Gobierno, a propuesta del Ministerio de Educación, Cultura y Deporte, al contemplarse la posibilidad de una formación profesional reglada o de grado universitario para el acceso a las diferentes profesiones de seguridad privada, o de los correspondientes certificados de profesionalidad del Ministerio de Empleo y Seguridad Social.

En el título IV se regulan por primera vez en una norma de rango legal y de forma armónica las medidas de seguridad, así como la especificación de la forma de prestación de los principales servicios de seguridad (vigilancia y protección, protección personal, depósitos y transportes de seguridad, e investigación privada), dotando de concreción a otros importantes servicios para los que la Ley 23/1992, de 30 de julio, y su reglamento de desarrollo no contienen más que referencias aisladas (verificación y respuesta ante alarmas, instalación y mantenimiento de sistemas), o no contienen regulación alguna, como sucede con la videovigilancia en el ámbito de la seguridad privada, en cumplimiento del mandato contenido en la Ley Orgánica 4/1997, de 4 de agosto, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

En este título resulta especialmente relevante la regulación de los servicios de videovigilancia y de investigación privada, ya que se trata de servicios que potencialmente pueden incidir de forma directa en la esfera de la intimidad de los ciudadanos. En el segundo caso, desde el ánimo de compaginar los diversos intereses en juego, se abordan cuestiones tan delicadas como la legitimidad del encargo, el contenido del informe de investigación o el deber de reserva profesional.

En el título V se recogen, también por vez primera en sede legal, las actuaciones de control e inspección sobre las entidades, el personal y las medidas de seguridad, así como la obligación de colaboración por parte de los afectados. Especialmente relevante es la incorporación de un precepto que regula las medidas provisionales que pueden adoptar los funcionarios policiales, cuando en el marco de una inspección lo consideren absolutamente necesario, quedando en todo caso sujetas a ratificación por la autoridad competente. Igualmente, se limita, por razón de la intimidad de los datos, el acceso al contenido de los informes de investigación privada en las inspecciones policiales a la mera constatación de su existencia, salvo que medien investigaciones policiales o judiciales o procedimientos sancionadores.

En el título VI se da solución a algunas de las principales carencias de la anterior legislación referidas al régimen sancionador. Así, se contemplan con la debida separación las infracciones que pueden ser cometidas por las entidades, el personal o los usuarios de seguridad privada, incluyendo, junto a estos últimos, a los centros de formación en la materia.

Se hace especial hincapié en la regulación de todas aquellas conductas infractoras que tengan por objeto evitar el intrusismo ya sea realizado por empresas de seguridad, por personal no habilitado, por empresas de servicios que desarrollan actividades materialmente de seguridad privada o por los propios usuarios.

A este respecto, es importante destacar el esfuerzo que se ha hecho en cuanto a la graduación de las infracciones y a los criterios para determinar la imposición de las correspondientes sanciones, con el objetivo básico de garantizar la mayor individualización de aquéllas.

Por último, en la parte final, el texto contempla aquellas disposiciones necesarias para garantizar una transición correcta desde la Ley 23/1992, de 30 de julio, a la nueva legislación, sobre todo hasta que ésta sea objeto del correspondiente desarrollo reglamentario.

TÍTULO PRELIMINAR

Disposiciones generales

CAPÍTULO I

Disposiciones comunes

Artículo 1. *Objeto.*

1. Esta ley tiene por objeto regular la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y servicios de seguridad privada que, desarrollados por éstos, son contratados, voluntaria u obligatoriamente, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Igualmente regula las investigaciones privadas que se efectúen sobre aquéllas o éstos. Todas estas actividades tienen la consideración de complementarias y subordinadas respecto de la seguridad pública.

2. Asimismo, esta ley, en beneficio de la seguridad pública, establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios.

Artículo 2. *Definiciones.*

A los efectos de esta ley se entiende por:

1. Seguridad privada: el conjunto de actividades, servicios, funciones y medidas de seguridad adoptadas, de forma voluntaria u obligatoria, por personas físicas o jurídicas, públicas o privadas, realizadas o prestados por empresas de seguridad, despachos de detectives privados y personal de seguridad privada para hacer frente a actos deliberados o riesgos accidentales, o para realizar averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades.

2. Actividades de seguridad privada: los ámbitos de actuación material en que los prestadores de servicios de seguridad privada llevan a cabo su acción empresarial y profesional.

3. Servicios de seguridad privada: las acciones llevadas a cabo por los prestadores de servicios de seguridad privada para materializar las actividades de seguridad privada.

4. Funciones de seguridad privada: las facultades atribuidas al personal de seguridad privada.

5. Medidas de seguridad privada: las disposiciones adoptadas para el cumplimiento de los fines de prevención o protección pretendidos.

6. Prestadores de servicios de seguridad privada: las empresas de seguridad privada, los despachos de detectives y el personal habilitado para el ejercicio de funciones de seguridad privada.

7. Empresa de seguridad privada: las personas físicas o jurídicas, privadas, autorizadas o sometidas al régimen de declaración responsable, para prestar servicios de seguridad privada.

8. Personal de seguridad privada: las personas físicas que, habiendo obtenido la correspondiente habilitación, desarrollan funciones de seguridad privada.

9. Personal acreditado: profesores de centros de formación, ingenieros y técnicos que desarrollen las tareas que les asignan esta ley y operadores de seguridad.

10. Usuario de seguridad privada: las personas físicas o jurídicas que, de forma voluntaria u obligatoria, contratan servicios o adoptan medidas de seguridad privada.

11. Despachos de detectives privados: las oficinas constituidas por uno o más detectives privados que prestan servicios de investigación privada.

12. Centros de formación de aspirantes o de personal de seguridad privada: establecimientos sometidos al régimen de declaración responsable para impartir en sus locales formación al personal de seguridad privada.

13. Elemento, producto o servicio homologado: aquel que reúne las especificaciones técnicas o criterios que recoge una norma técnica al efecto.

14. Elemento, producto o servicio acreditado, certificado o verificado: aquel que lo ha sido por una entidad independiente, constituida a tal fin y reconocida por cualquier Estado miembro de la Unión Europea.

Artículo 3. *Ámbito de aplicación.*

1. Las disposiciones de esta ley son de aplicación a las empresas de seguridad privada, al personal de seguridad privada, a los despachos de detectives, a los servicios de seguridad privada, a las medidas de seguridad y a los contratos celebrados en éste ámbito.

2. Igualmente, en la medida que resulte pertinente en cada caso, se aplicarán a los establecimientos obligados a disponer de medidas de seguridad, a los usuarios de los servicios de seguridad privada, a los ingenieros y técnicos de las empresas de seguridad, a los operadores de seguridad, a los profesores de centros de formación, a las empresas prestadoras de servicios de seguridad informática, a las centrales receptoras de alarmas de uso propio y a los centros de formación de personal de seguridad privada.

3. El régimen sancionador y las medidas provisionales, así como el ejercicio de las facultades de inspección, serán también aplicables a aquellas empresas y personal que presten servicios o ejerzan funciones de seguridad privada sin estar autorizadas o haber presentado declaración responsable, o sin estar habilitados o acreditados para el ejercicio legal de los mismos.

Artículo 4. *Fines.*

La seguridad privada tiene como fines:

a) Satisfacer las necesidades legítimas de seguridad o de información de los usuarios de seguridad privada, velando por la indemnidad o privacidad de las personas o bienes cuya seguridad o investigación se le encomiende frente a posibles vulneraciones de derechos, amenazas deliberadas y riesgos accidentales o derivados de la naturaleza.

b) Contribuir a garantizar la seguridad pública, a prevenir infracciones y a aportar información a los procedimientos relacionados con sus actuaciones e investigaciones.

c) Complementar el monopolio de la seguridad que corresponde al Estado, integrando funcionalmente sus medios y capacidades como un recurso externo de la seguridad pública.

Artículo 5. *Actividades de seguridad privada.*

1. Constituyen actividades de seguridad privada las siguientes:

a) La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos.

b) El acompañamiento, defensa y protección de personas físicas determinadas, incluidas las que ostenten la condición legal de autoridad.

c) El depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, joyas, metales preciosos, antigüedades, obras de arte u otros objetos que, por su valor económico, histórico o cultural, y expectativas que generen, puedan requerir vigilancia y protección especial.

d) El depósito y custodia de explosivos, armas, cartuchería metálica, sustancias, materias, mercancías y cualesquiera objetos que por su peligrosidad precisen de vigilancia y protección especial.

e) El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores.

f) La instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia.

g) La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de

cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos.

h) La investigación privada en relación a personas, hechos o delitos sólo perseguibles a instancia de parte.

2. Los servicios sobre las actividades relacionadas en los párrafos a) a g) del apartado anterior únicamente podrán prestarse por empresas de seguridad privada, sin perjuicio de las competencias de las Fuerzas y Cuerpos de Seguridad. Los despachos de detectives podrán prestar, con carácter exclusivo y excluyente, servicios sobre la actividad a la que se refiere el párrafo h) del apartado anterior.

3. Las entidades públicas o privadas podrán constituir, previa autorización del Ministerio del Interior o del órgano autonómico competente, centrales receptoras de alarmas de uso propio para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma que reciban de los sistemas de seguridad instalados en bienes inmuebles o muebles de su titularidad, sin que puedan dar, a través de las mismas, ningún tipo de servicio de seguridad a terceros.

Artículo 6. *Actividades compatibles.*

1. Quedan fuera del ámbito de aplicación de esta ley, sin perjuicio de la normativa específica que pudiera resultar de aplicación, especialmente en lo que se refiere a la homologación de productos, las siguientes actividades:

a) La fabricación, comercialización, venta, entrega, instalación o mantenimiento de elementos o productos de seguridad y de cerrajería de seguridad.

b) La fabricación, comercialización, venta o entrega de equipos técnicos de seguridad electrónica, así como la instalación o mantenimiento de dichos equipos siempre que no estén conectados a centrales de alarma o centros de control o de videovigilancia.

c) La conexión a centrales receptoras de alarmas de sistemas de prevención o protección contra incendios o de alarmas de tipo técnico o asistencial, o de sistemas o servicios de control o mantenimiento.

d) La planificación, consultoría y asesoramiento en materia de actividades de seguridad privada, que consistirá en la elaboración de estudios e informes de seguridad, análisis de riesgos y planes de seguridad referidos a la protección frente a todo tipo de riesgos, así como en auditorías sobre la prestación de los servicios de seguridad.

Estas actividades podrán desarrollarse por las empresas de seguridad privada.

2. Quedan también fuera del ámbito de aplicación de esta ley, a no ser que impliquen la asunción o realización de servicios o funciones de seguridad privada, y se regirán por las normas sectoriales que les sean de aplicación en cada caso, los siguientes servicios y funciones:

a) Las de información o de control en los accesos a instalaciones, comprendiendo el cuidado y custodia de las llaves, la apertura y cierre de puertas, la ayuda en el acceso de personas o vehículos, el cumplimiento de la normativa interna de los locales donde presten dicho servicio, así como la ejecución de tareas auxiliares o subordinadas de ayuda o socorro, todas ellas realizadas en las puertas o en el interior de inmuebles, locales públicos, aparcamientos, garajes, autopistas, incluyendo sus zonas de peajes, áreas de servicio, mantenimiento y descanso, por porteros, conserjes y demás personal auxiliar análogo.

b) Las tareas de recepción, comprobación de visitantes y orientación de los mismos, así como las de comprobación de entradas, documentos o carnés, en cualquier clase de edificios o inmuebles, y de cumplimiento de la normativa interna de los locales donde presten dicho servicio.

c) El control de tránsito en zonas reservadas o de circulación restringida en el interior de instalaciones en cumplimiento de la normativa interna de los mismos.

d) Las de comprobación y control del estado y funcionamiento de calderas, bienes e instalaciones en general, en cualquier clase de inmuebles, para garantizar su conservación y funcionamiento.

Estos servicios y funciones podrán prestarse o realizarse por empresas y personal de seguridad privada, siempre con carácter complementario o accesorio de las funciones de seguridad privada que se realicen y sin que en ningún caso constituyan el objeto principal del servicio que se preste.

3. El personal no habilitado que preste los servicios o funciones comprendidos en el apartado anterior, en ningún caso podrá ejercer función alguna de las reservadas al personal de seguridad privada, ni portar ni usar armas ni medios de defensa, ni utilizar distintivos, uniformes o medios que puedan confundirse con los previstos para dicho personal.

4. Los prestadores de servicios de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, no conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia, quedan fuera del ámbito de aplicación de la legislación de seguridad privada.

5. Las empresas de seguridad privada que se dediquen a la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que no incluyan la conexión a centrales receptoras de alarmas o a centros de control o de videovigilancia, sólo están sometidas a la normativa de seguridad privada en lo que se refiere a las actividades y servicios de seguridad privada para las que se encontrasen autorizadas.

6. A las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática, entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan, por su incidencia directa en la seguridad de las entidades públicas y privadas, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten.

Artículo 7. *Actividades excluidas.*

1. No están sujetas a esta ley las actuaciones de autoprotección, entendidas como el conjunto de cautelas o diligencias que se puedan adoptar o que ejecuten por sí y para sí mismos de forma directa los interesados, estrictamente dirigidas a la protección de su entorno personal o patrimonial, y cuya práctica o aplicación no conlleve contraprestación alguna ni suponga algún tipo de servicio de seguridad privada prestado a terceros.

Cuando los interesados tengan el carácter de empresas o entidades de cualquier tipo, en ningún caso utilizarán a sus empleados para el desarrollo de las funciones previstas en la presente ley, reservadas a las empresas y el personal de seguridad privada.

2. Queda fuera del ámbito de aplicación de esta ley la obtención por uno mismo de información o datos, así como la contratación de servicios de recepción, recopilación, análisis, comunicación o suministro de información libre obrante en fuentes o registros de acceso público.

Artículo 8. *Principios rectores.*

1. Los servicios y funciones de seguridad privada se prestarán con respeto a la Constitución, a lo dispuesto en esta ley, especialmente en lo referente a los principios de actuación establecidos en el artículo 30, y al resto del ordenamiento jurídico.

2. Los prestadores de servicios de seguridad privada colaborarán, en todo momento y lugar, con las Fuerzas y Cuerpos de Seguridad, con sujeción a lo que éstas puedan disponer en relación con la ejecución material de sus actividades.

3. De conformidad con lo dispuesto en la legislación de fuerzas y cuerpos de seguridad, las empresas de seguridad, los despachos de detectives y el personal de seguridad privada tendrán especial obligación de auxiliar y colaborar, en todo momento, con aquéllas en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones, en relación con los servicios que presten que afecten a la seguridad pública o al ámbito de sus competencias.

4. Las empresas, los despachos y el personal de seguridad privada:

a) No podrán intervenir ni interferir, mientras estén ejerciendo los servicios y funciones que les son propios, en la celebración de reuniones y manifestaciones, ni en el desarrollo de conflictos políticos o laborales.

b) No podrán ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas, o sobre la expresión de tales opiniones, ni proceder al tratamiento, automatizado o no, de datos relacionados con la ideología, afiliación sindical, religión o creencias.

c) Tendrán prohibido comunicar a terceros, salvo a las autoridades judiciales y policiales para el ejercicio de sus respectivas funciones, cualquier información que conozcan en el desarrollo de sus servicios y funciones sobre sus clientes o personas relacionadas con éstos, así como sobre los bienes y efectos de cuya seguridad o investigación estuvieran encargados.

5. El Ministro del Interior o, en su caso, el titular del órgano autonómico competente prohibirá la utilización en los servicios de seguridad privada de determinados medios materiales o técnicos cuando pudieran causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana.

6. Cuando el personal de seguridad privada desempeñe sus funciones en entidades públicas o privadas en las que se presten servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los que el servicio de seguridad se haya impuesto obligatoriamente, habrán de atenerse, en el ejercicio del derecho de huelga, a lo que respecto de dichas entidades disponga la legislación vigente.

Artículo 9. *Contratación y comunicación de servicios.*

1. No podrá prestarse ningún tipo de servicio de seguridad privada que no haya sido previamente contratado y, en su caso, autorizado.

2. De acuerdo con lo que reglamentariamente se determine, los contratos de prestación de los distintos servicios de seguridad privada deberán, en todo caso, formalizarse por escrito y comunicarse su celebración al Ministerio del Interior o, en su caso, al órgano autonómico competente con antelación a la iniciación de los mismos.

3. La comunicación de contratos de servicios de investigación privada contendrá exclusivamente los datos necesarios para identificar a las partes contratantes, excluidos los de carácter personal.

Artículo 10. *Prohibiciones.*

1. Con carácter general y además de otras prohibiciones contenidas en esta ley, se establecen las siguientes:

a) La prestación o publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

b) El ejercicio de funciones de seguridad privada por parte de personas físicas carentes de la correspondiente habilitación o acreditación profesional.

c) La prestación de servicios de seguridad privada incumpliendo los requisitos o condiciones legales de prestación de los mismos.

d) El empleo o utilización, en servicios de seguridad privada, de medios o medidas de seguridad no homologadas cuando sea preceptivo, o de medidas o medios personales, materiales o técnicos de forma tal que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, o cuando incumplan las condiciones o requisitos establecidos en esta ley y en su normativa de desarrollo.

2. Los despachos de detectives y los detectives privados no podrán celebrar contratos que tengan por objeto la investigación de delitos perseguibles de oficio ni, en general, investigar delitos de esta naturaleza, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento, relacionado con dichos delitos.

3. Las empresas de seguridad no podrán realizar los servicios de investigación privada propios de los despachos de detectives privados, y éstos no podrán prestar servicios propios de las empresas de seguridad privada.

Artículo 11. *Registro Nacional de Seguridad Privada y registros autonómicos.*

1. Serán objeto de inscripción de oficio en el Registro Nacional de Seguridad Privada del Ministerio del Interior, una vez concedidas las pertinentes autorizaciones o, en su caso, presentadas las declaraciones responsables, u obtenidas las preceptivas habilitaciones o acreditaciones, el personal de seguridad privada, las empresas de seguridad privada y los despachos de detectives privados, así como delegaciones y sucursales, los centros de formación del personal de seguridad privada y las centrales receptoras de alarma de uso propio, cuando no sean objeto de inscripción en los registros de las comunidades autónomas.

Igualmente, se inscribirán en el Registro Nacional de Seguridad Privada las sanciones impuestas en materia de seguridad privada, las comunicaciones de los contratos y sus modificaciones y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada, cuando tales sanciones, comunicaciones y datos se refieran a servicios de seguridad privada que se presten en un ámbito territorial distinto al de una comunidad autónoma con competencia en materia de seguridad privada.

2. En los registros de las comunidades autónomas, una vez concedidas las pertinentes autorizaciones o, en su caso, presentadas las declaraciones responsables, u obtenidas las preceptivas habilitaciones, se inscribirán de oficio las empresas de seguridad privada y los despachos de detectives privados, así como delegaciones y sucursales, los centros de formación del personal de seguridad privada y las centrales receptoras de alarma de uso propio, que tengan su domicilio en la comunidad autónoma y cuyo ámbito de actuación esté limitado a su territorio.

Igualmente, se inscribirán en dichos registros las sanciones impuestas en materia de seguridad privada, las comunicaciones de los contratos y sus modificaciones y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada, cuando tales sanciones, comunicaciones y datos se refieran a servicios de seguridad privada que se presten en el ámbito territorial propio de una comunidad autónoma con competencia en materia de seguridad privada.

3. En el referido Registro Nacional, además de la información correspondiente a las empresas de seguridad privada que en el mismo se inscriban, se incorporará la relativa a las empresas de seguridad privada inscritas en los registros de las comunidades autónomas con competencia en la materia.

A tales efectos, los órganos competentes de las mencionadas comunidades autónomas deberán comunicar al Registro Nacional de Seguridad Privada los datos de las inscripciones y anotaciones que efectúen sobre las empresas de seguridad privada que inscriban, así como sus modificaciones y cancelaciones.

4. En los mencionados registros, nacional y autonómicos, se anotarán también los datos de las empresas que realicen actividades de seguridad informática, de acuerdo con lo que reglamentariamente se determine.

5. Las autoridades responsables del Registro Nacional y de los registros autonómicos establecerán los mecanismos de colaboración y reciprocidad necesarios para permitir su interconexión e interoperabilidad, la determinación coordinada de los sistemas de numeración de las empresas de seguridad privada y el acceso a la información registral contenida en los mismos, para el ejercicio de sus respectivas competencias.

6. Dichos registros serán públicos exclusivamente en cuanto a los asientos referentes a la denominación o razón social, domicilio, número de identificación fiscal y actividades en relación con las cuales estén autorizadas o hayan presentado la declaración responsable las empresas de seguridad privada, despachos de detectives, centros de formación del personal de seguridad privada y centrales de alarmas de uso propio.

7. Reglamentariamente se regulará la organización y funcionamiento del Registro Nacional de Seguridad Privada.

CAPÍTULO II

Competencias de la Administración General del Estado y de las comunidades autónomas

Artículo 12. *Competencias de la Administración General del Estado.*

1. Corresponde a la Administración General del Estado, a través del Ministerio del Interior y, en su caso, de las Delegaciones y Subdelegaciones del Gobierno, el ejercicio de las siguientes facultades:

a) La autorización o recepción de la declaración responsable, inspección y sanción de las empresas de seguridad privada y de sus delegaciones cuya competencia no haya sido asumida por las comunidades autónomas.

b) La recepción de la declaración responsable para la apertura de los despachos de detectives privados y de sus sucursales, así como su inspección y sanción, cuando el ejercicio de estas facultades no sea competencia de las comunidades autónomas.

c) La habilitación e inhabilitación del personal de seguridad privada, y la determinación del armamento, documentación, uniformidad, distintivos y medios de defensa de dicho personal, así como la acreditación, en todo caso, de los ingenieros y técnicos de las empresas de seguridad y de los operadores de seguridad.

d) La aprobación, modificación y cancelación de los programas y cursos específicos de formación del personal de seguridad privada que no sean de la competencia de los Ministerios de Educación, Cultura y Deporte o de Empleo y Seguridad Social.

e) La recepción de la declaración responsable, inspección y sanción de los centros de formación del personal de seguridad privada cuya competencia no haya sido asumida por las comunidades autónomas, así como la acreditación, en todo caso, de su profesorado.

f) La autorización, inspección y sanción de los servicios de protección personal, cuando no sea competencia de las comunidades autónomas, y de aquellas actividades y servicios transfronterizos de seguridad que puedan prestarse por las empresas y el personal de seguridad privada.

g) La autorización de los servicios de seguridad privada y de centrales de alarma de uso propio que se presten en un ámbito territorial superior al de una comunidad autónoma con competencia en materia de seguridad privada, así como la inspección y sanción de estos servicios en aquella parte de los mismos que se realice fuera del territorio de dichas comunidades autónomas.

h) La determinación reglamentaria de las características técnicas y de homologación que resulten exigibles a los productos, sistemas, dispositivos, equipos, medidas y servicios de seguridad privada.

i) La determinación reglamentaria de los establecimientos obligados a disponer de medidas de seguridad privada, así como la fijación del tipo y alcance de las medidas obligatorias que ha de cumplir cada tipo de establecimiento.

j) La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios que estén obligados a adoptar medidas de seguridad, cuando el ejercicio de esas facultades no sea competencia de las comunidades autónomas.

k) La coordinación de los servicios de seguridad e investigación privadas con los de las Fuerzas y Cuerpos de Seguridad del Estado.

2. En el ámbito de las competencias de la Administración General del Estado y de conformidad con lo dispuesto en la legislación de Fuerzas y Cuerpos de Seguridad:

a) Corresponde a la Dirección General de la Policía el control de las empresas, entidades y servicios privados de seguridad, vigilancia e investigación, de su personal, medios y actuaciones.

b) Corresponde a la Dirección General de la Guardia Civil el ejercicio de sus competencias en materia de armas sobre las empresas y el personal de seguridad privada, así como el control de los guardas rurales y sus especialidades. Sin afectar a las competencias que corresponden a la Dirección General de la Policía podrá participar en el

control de las actuaciones operativas del personal de seguridad privada, que preste servicios en su ámbito de competencias.

Artículo 13. *Competencias de las comunidades autónomas.*

1. Las comunidades autónomas que, con arreglo a sus estatutos de autonomía, tengan competencia para la protección de personas y bienes y para el mantenimiento del orden público, ejecutarán la legislación del Estado sobre las siguientes materias:

a) La autorización de las empresas de seguridad privada y de sus delegaciones, así como la recepción de la declaración responsable para la apertura de los despachos de detectives privados y de sus sucursales, cuando, en ambos casos, tengan su domicilio en la comunidad autónoma y su ámbito de actuación esté limitado a su territorio.

b) La autorización de las actividades y servicios de seguridad privada que se realicen en la comunidad autónoma cuando requieran de la misma o de control previo.

c) La inspección y sanción de las actividades y servicios de seguridad privada que se realicen en la comunidad autónoma, así como de quienes los presten o utilicen y la inspección y sanción de los despachos de detectives privados y de sus sucursales que realicen su actividad en la comunidad autónoma.

d) La recepción de la declaración responsable, inspección y sanción de los centros de formación del personal de seguridad privada que tengan su sede en la comunidad autónoma.

e) La coordinación de los servicios de seguridad e investigación privadas prestados en la comunidad autónoma con los de la policía autonómica y las policías locales.

f) La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios sitos en la comunidad autónoma que estén obligados a adoptar medidas de seguridad.

2. Las comunidades autónomas que, en virtud de sus estatutos de autonomía, hayan asumido competencia ejecutiva en materia de seguridad privada cuando así lo establezca la legislación del Estado, la ejercerán si disponen de cuerpo de policía propia o establecen fórmulas de colaboración con el Cuerpo Nacional de Policía previstas en la legislación de fuerzas y cuerpos de seguridad, sobre las siguientes materias:

a) La autorización, inspección y sanción de las empresas de seguridad privada que tengan su domicilio en la comunidad autónoma y cuyo ámbito de actuación esté limitado a su territorio.

b) La denuncia, y puesta en conocimiento de las autoridades competentes, de las infracciones cometidas por las empresas de seguridad que no se encuentren incluidas en el párrafo anterior.

TÍTULO I

Coordinación

Artículo 14. *Colaboración profesional.*

1. La especial obligación de colaboración de las empresas de seguridad, los despachos de detectives y el personal de seguridad privada con las Fuerzas y Cuerpos de Seguridad se desarrollará con sujeción al principio de legalidad y se basará exclusivamente en la necesidad de asegurar el buen fin de las actuaciones tendentes a preservar la seguridad pública, garantizándose la debida reserva y confidencialidad cuando sea necesario.

2. Las empresas de seguridad, los despachos de detectives y el personal de seguridad privada deberán comunicar a las Fuerzas y Cuerpos de Seguridad competentes, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo del que tuviesen conocimiento en el ejercicio de su actividad o funciones, poniendo a su disposición a los presuntos delincuentes, así como los instrumentos, efectos y pruebas relacionadas con los mismos.

3. Las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección. Si estas informaciones contuvieran datos de carácter personal sólo podrán facilitarse en caso de peligro real para la seguridad pública o para evitar la comisión de infracciones penales.

Artículo 15. *Acceso a la información por las Fuerzas y Cuerpos de Seguridad.*

1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Artículo 16. *Coordinación y participación.*

1. El Ministerio del Interior o, en su caso, el órgano autonómico competente adoptará las medidas organizativas que resulten adecuadas para asegurar la coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad.

2. En el ámbito de las competencias de la Administración General del Estado se constituirán comisiones mixtas de seguridad privada, nacionales, autonómicas o provinciales, con el carácter de órganos consultivos y de colaboración entre las administraciones públicas y los representantes del sector. Su composición y funciones se determinarán reglamentariamente.

3. En las comunidades autónomas que tengan asumidas las competencias en materia de seguridad privada de conformidad con lo establecido en el artículo 13, también podrán existir órganos consultivos en materia de seguridad privada, con la composición y funcionamiento que en cada caso se determine.

TÍTULO II

Empresas de seguridad privada y despachos de detectives privados

CAPÍTULO I

Empresas de seguridad privada

Artículo 17. *Desarrollo de actividades.*

1. Las empresas de seguridad privada únicamente podrán prestar servicios sobre las actividades previstas en el artículo 5.1, excepto la contemplada en el párrafo h) del mismo.

2. Además de estas actividades, las empresas de seguridad privada podrán realizar las actividades compatibles a las que se refiere el artículo 6 y dedicarse a la formación, actualización y especialización del personal de seguridad privada, perteneciente o no a sus plantillas, en cuyo caso deberán crear centros de formación, de conformidad con lo previsto en el artículo 29.4 y a lo que reglamentariamente se determine.

3. Las empresas de seguridad privada podrán revestir forma societaria o de empresario individual, debiendo cumplir, en ambos casos, la totalidad de condiciones y requisitos previstos en este capítulo para las empresas de seguridad privada.

Artículo 18. *Autorización administrativa.*

1. Para la prestación de servicios de seguridad privada, las empresas de seguridad privada deberán obtener autorización administrativa y serán inscritas de oficio en el registro correspondiente, de acuerdo con el procedimiento que se determine reglamentariamente.

2. La autorización administrativa se suplirá por una declaración responsable cuando pretendan dedicarse exclusivamente a la actividad de seguridad privada contemplada en el artículo 5.1.f).

3. La validez de la autorización o de la declaración responsable será indefinida.

Artículo 19. *Requisitos generales.*

1. Para la autorización o, en su caso, presentación de declaración responsable, la posterior inscripción en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico y el desarrollo de servicios de seguridad privada, las empresas de seguridad privada deberán reunir los siguientes requisitos generales:

a) Estar legalmente constituidas e inscritas en el registro mercantil o en el registro público correspondiente y tener por objeto exclusivo todas o alguna de las actividades a las que se refiere el artículo 5.1, excepto la del párrafo h). No obstante, en dicho objeto podrán incluir las actividades que resulten imprescindibles para el cumplimiento de las actividades de seguridad autorizadas, así como las compatibles contempladas en el artículo 6.

b) Tener la nacionalidad de un Estado miembro de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

c) Contar con los medios humanos, de formación, financieros, materiales y técnicos adecuados que, de acuerdo con el principio de proporcionalidad, se determinen reglamentariamente, en función de la naturaleza de las actividades para las que soliciten la autorización o se presente la declaración responsable, y de las características de los servicios que se prestan en relación con tales actividades. En particular, cuando se presten servicios para los que se precise el uso de armas, habrán de adoptarse las medidas que garanticen su adecuada custodia, utilización y funcionamiento. Igualmente, los ingenieros y técnicos de las empresas de seguridad privada y los operadores de seguridad, deberán disponer de la correspondiente acreditación expedida por el Ministerio del Interior, que se limitará a comprobar la honorabilidad del solicitante y la carencia de antecedentes penales, en los términos que reglamentariamente se establezca.

d) Disponer de las medidas de seguridad que reglamentariamente se determinen.

e) Suscribir un contrato de seguro de responsabilidad civil o constituir otras garantías financieras en la cuantía y con las condiciones que se determinen reglamentariamente.

f) Constituir el aval o seguro de caución que se determine reglamentariamente a disposición de las autoridades españolas, para atender exclusivamente las responsabilidades administrativas por infracciones a la normativa de seguridad privada que se deriven del funcionamiento de la empresa.

g) No haber sido condenadas mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social, contra los derechos de los trabajadores, por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales, salvo que hubiesen cancelado sus antecedentes penales. En el caso de las personas jurídicas, este requisito será aplicable a los administradores de hecho o de derecho y representantes, que, vigente su cargo o representación, no podrán estar incursos en la situación mencionada por actuaciones realizadas en nombre o a beneficio de dichas personas jurídicas.

h) No haber sido condenadas mediante sentencia firme por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud. En el caso de las personas jurídicas, este requisito

será aplicable a los administradores de hecho o de derecho y representantes, que, vigente su cargo o representación, no podrán estar incursos en la situación mencionada por actuaciones realizadas en nombre o a beneficio de dichas personas jurídicas.

2. Además del cumplimiento de los requisitos generales, a las empresas de seguridad privada que tengan por objeto alguna de las actividades contempladas en el artículo 5.1.b), c), d), e) y g), se les podrá exigir reglamentariamente el cumplimiento de requisitos y garantías adicionales adecuados a la singularidad de los servicios relacionados con dichas actividades.

3. Igualmente, en relación con las actividades contempladas en el artículo 5.1.a), f) y g), podrán ampliarse los requisitos referentes a medios personales y materiales, conforme se disponga reglamentariamente, para poder prestar servicios de seguridad privada en infraestructuras críticas o en servicios esenciales, así como en los servicios descritos en el artículo 40.1 y en artículo 41.2 y 3.

4. Para la contratación de servicios de seguridad privada en los sectores estratégicos definidos en la legislación de protección de infraestructuras críticas, las empresas de seguridad privada deberán contar, con carácter previo a su prestación, con una certificación emitida por una entidad de certificación acreditada que garantice, como mínimo, el cumplimiento de la normativa administrativa, laboral, de Seguridad Social y tributaria que les sea de aplicación.

5. A los efectos previstos en el apartado 1.e) y f), de este artículo se tendrán en cuenta los requisitos ya exigidos en el Estado miembro de la Unión Europea o parte en el Acuerdo sobre el Espacio Económico Europeo de origen en lo referente a la suscripción del contrato de seguro de responsabilidad civil u otras garantías financieras, así como a la constitución de avales o seguros de caución.

6. Las empresas de seguridad privada no españolas, autorizadas para la prestación de servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión Europea o de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, habrán de inscribirse obligatoriamente en el Registro Nacional de Seguridad Privada del Ministerio del Interior o, cuando tengan su domicilio en una comunidad autónoma con competencias en materia de seguridad privada y su ámbito de actuación limitado a dicho territorio, en el registro autonómico correspondiente, a cuyo efecto deberán acreditar su condición de empresas de seguridad privada y el cumplimiento de los requisitos establecidos en esta ley, en la forma que se determine reglamentariamente.

7. Sin perjuicio de lo dispuesto en los apartados anteriores, a las empresas de seguridad privada que tengan por objeto exclusivo la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que incluyan la prestación de servicios de conexión con centrales receptoras de alarma se las podrá eximir del cumplimiento de alguno de los requisitos incluidos en este artículo, excepto los contemplados en los párrafos e) y f) del apartado 1, cuando así se determine reglamentariamente.

8. El incumplimiento sobrevenido de los requisitos establecidos en este artículo dará lugar a la extinción de la autorización o al cierre de la empresa, en el caso de presentación de declaración responsable, y, en ambos casos, a la cancelación de oficio de la inscripción de la empresa de seguridad en el registro correspondiente.

Artículo 20. *Inscripción registral.*

1. Toda empresa de seguridad privada autorizada o que, en su caso, haya presentado la correspondiente declaración responsable será inscrita de oficio en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico.

2. No podrá inscribirse en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico ninguna empresa cuya denominación coincida, o pueda inducir a error o confusión, con la de otra ya inscrita o con la de órganos o dependencias de las administraciones públicas, o cuando coincida o pueda inducir a confusión con una marca anterior registrada para actividades idénticas o semejantes, salvo que se solicite por el titular de la misma o con su consentimiento.

Artículo 21. *Obligaciones generales.*

1. Las empresas de seguridad privada deberán cumplir las siguientes obligaciones generales:

a) Desarrollar las actividades de seguridad privada en los términos de esta ley y en las condiciones establecidas en la autorización que les haya sido concedida o en la declaración responsable que hayan presentado.

b) Contar con la infraestructura y logística acorde con las exigencias establecidas en esta ley y en su desarrollo reglamentario.

c) Comunicar al Registro Nacional o autonómico correspondiente todo cambio que se produzca en cuanto a su forma jurídica, denominación, número de identificación fiscal, domicilio, delegaciones, ámbito territorial de actuación, representantes legales, estatutos, titularidad de las acciones y participaciones sociales, y toda variación que sobrevenga en la composición de los órganos de administración, gestión, representación y dirección de las empresas.

Las empresas de seguridad deben comunicar al Registro Nacional o autonómico del lugar donde presten servicios las altas y bajas del personal de seguridad privada de que dispongan y las incidencias concretas relacionadas con los servicios que prestan.

d) Garantizar la formación y actualización profesional del personal de seguridad privada del que dispongan y del personal de la empresa que requiera formación en materia de seguridad privada. El mantenimiento de la aptitud en el uso de las armas de fuego se hará con la participación de instructores de tiro habilitados.

e) Presentar cada año al Ministerio del Interior o al órgano autonómico competente un informe sobre sus actividades y el resumen de las cuentas anuales, debidamente auditadas cuando sea preceptivo, con la información y datos que reglamentariamente se determinen. En ningún caso dicha memoria contendrá datos de carácter personal. El Ministerio del Interior y los órganos autonómicos competentes darán cuenta del funcionamiento del sector a las Cortes Generales y a los Parlamentos autonómicos correspondientes respectivamente, anualmente.

2. Asimismo, las empresas de seguridad privada vendrán obligadas a prestar especial auxilio y colaboración a las Fuerzas y Cuerpos de Seguridad, debiendo facilitar a éstas la información que se les requiera en relación con las competencias atribuidas a las mismas.

Artículo 22. *Representantes legales.*

1. A los efectos de esta ley, se entenderá por representante legal de las empresas de seguridad privada todo aquel que asuma o realice las tareas de dirección, administración, gestión y representación, o cualquiera de ellas, en nombre de aquéllas.

2. Los representantes de las empresas de seguridad privada, que se inscribirán en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico, deberán:

a) Ser personas físicas residentes en el territorio de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

b) Carecer de antecedentes penales por delitos dolosos.

c) No haber sido sancionados en los dos o cuatro años anteriores por infracción grave o muy grave, respectivamente, en materia de seguridad privada.

d) No haber sido separados del servicio en las Fuerzas Armadas o en las Fuerzas y Cuerpos de Seguridad, ni haber ejercido funciones de control de las entidades o servicios de seguridad, vigilancia o investigación privadas, ni de su personal o medios, como miembros de las Fuerzas y Cuerpos de Seguridad, en los dos años anteriores.

e) No haber sido administrador de hecho o de derecho o apoderado general, en los diez años anteriores, en una empresa que haya sido declarada en concurso calificado como culpable, o condenada mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social o contra los derechos de los trabajadores, por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal

y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales.

3. Los representantes legales de las empresas de seguridad privada serán responsables del cumplimiento de las obligaciones generales impuestas a las mismas por el artículo anterior.

Artículo 23. *Consideración de sector específico.*

1. Las empresas de seguridad privada tienen la consideración de sector económico con regulación específica en materia de derecho de establecimiento.

2. Cuando el Consejo de Ministros, con arreglo a lo dispuesto en la normativa sobre inversiones extranjeras, suspenda el régimen de liberalización de los movimientos de capital, la autorización previa de inversiones de capital extranjero en empresas de seguridad privada exigirá, en todo caso, informe previo del Ministerio del Interior.

3. Las empresas de seguridad privada en las que se hubieran realizado inversiones de capital extranjero estarán obligadas a comunicar al Ministerio del Interior todo cambio que se produzca en las mismas, en relación con lo establecido en el artículo 21.1.c).

4. Las limitaciones establecidas en los dos apartados precedentes no son de aplicación a las personas físicas nacionales de los Estados miembros de la Unión Europea ni a las empresas constituidas de conformidad con la legislación de un Estado miembro y cuya sede social, administración central o centro de actividad principal se encuentre dentro de la Unión Europea.

CAPÍTULO II

Despachos de detectives privados

Artículo 24. *Apertura de despachos de detectives privados.*

1. De acuerdo con lo que se disponga reglamentariamente, podrán abrir despachos de detectives privados y, en su caso, sucursales, las personas físicas habilitadas como tales y las personas jurídicas constituidas exclusivamente por detectives privados habilitados, que únicamente podrán desarrollar la actividad mencionada en el artículo 5.1.h).

2. Los despachos de detectives privados se inscribirán de oficio en el Registro Nacional de Seguridad Privada o, en su caso, en el registro de la comunidad autónoma competente, previa presentación de declaración responsable en la forma que reglamentariamente se determine, para lo cual deberán reunir los siguientes requisitos generales:

a) Tener por objeto de su actividad profesional la realización de los servicios de investigación privada a que se refiere el artículo 48.1 y conforme a lo establecido en el artículo 10 de esta ley en materia de prohibiciones.

b) En el caso de personas jurídicas, estar legalmente constituidas e inscritas en el Registro Mercantil o en el registro público correspondiente, y cumplir con los requisitos establecidos en el artículo 19.1.g) y h).

c) Fijar un domicilio como sede física del despacho en el que se desarrollará la actividad, se llevará el libro-registro y se encontrará el archivo de los expedientes de contratación y de los informes de investigación.

d) Facilitar una relación nominal de detectives privados adscritos al despacho como integrantes asociados o dependientes del mismo.

e) Suscribir un contrato de seguro de responsabilidad civil o constituir otras garantías financieras en la cuantía y con las condiciones que se determinen reglamentariamente.

f) Constituir el aval o seguro de caución que se determine reglamentariamente a disposición de las autoridades españolas para atender exclusivamente las responsabilidades administrativas por infracciones a la normativa de seguridad privada que se deriven del funcionamiento de los despachos.

g) Mantener en todo momento el titular y los demás detectives integrantes del despacho la habilitación profesional.

h) Contar con las medidas de seguridad que reglamentariamente se determinen.

3. La validez de la declaración responsable necesaria para la apertura de los despachos de detectives y de sus sucursales será indefinida.

4. Los despachos de detectives podrán revestir forma societaria o de empresario individual, debiendo, en ambos casos, cumplir la totalidad de requisitos y obligaciones previstos en este capítulo para los despachos de detectives.

5. El incumplimiento sobrevenido de los requisitos exigidos para la apertura de los despachos de detectives producirá el cierre de los mismos y la cancelación de oficio de su inscripción en el Registro Nacional de Seguridad Privada o, en su caso, en el registro de la comunidad autónoma competente.

Artículo 25. *Obligaciones generales.*

1. Los despachos de detectives privados y sus sucursales deberán cumplir las siguientes obligaciones generales:

a) Formalizar por escrito un contrato por cada servicio de investigación que les sea encargado, comunicando su celebración al Ministerio del Interior o, en su caso, al órgano autonómico competente en la forma que reglamentariamente se determine. Dicha obligación subsistirá igualmente en los casos de subcontratación entre despachos.

b) Llevar un libro-registro, con el formato que reglamentariamente se determine, en el que se anotará cada servicio de investigación contratado o subcontratado.

c) Informar a sus clientes sobre las incidencias relativas a los asuntos que les hubieren encargado, con entrega, en su caso, del informe de investigación elaborado.

d) Facilitar de forma inmediata a la autoridad judicial o a las Fuerzas y Cuerpos de Seguridad competentes las informaciones sobre hechos delictivos de que tuvieren conocimiento en relación con su trabajo o con las investigaciones que éstos estén llevando a cabo.

e) Acudir, cuando sean requeridos para ello por los órganos competentes de la Administración de Justicia y de las Fuerzas y Cuerpos de Seguridad, a su llamamiento, tan pronto como resulte posible, y facilitar las informaciones de que tuvieren conocimiento en relación con las investigaciones que tales organismos se encontraran llevando a cabo.

f) Atender las citaciones que realicen los juzgados y tribunales y las dependencias policiales, a los cuales sus informaciones hayan sido comunicadas o sus informes de investigación hayan sido aportados, para la prestación de testimonio y ratificación, en su caso, del contenido de los referidos informes de investigación.

g) Asegurar el archivo y conservación de la documentación relativa a su ejercicio profesional, especialmente de los contratos, informes, libros y material de imagen y sonido obtenido.

h) Comunicar al Ministerio del Interior o, en su caso, al órgano autonómico competente todo cambio que afecte a su forma jurídica, denominación, composición, domicilio y sucursales en la forma que reglamentariamente se determine.

i) Presentar al Ministerio del Interior o, en su caso, al órgano autonómico competente, una memoria anual de actividades del año precedente, con la información que se determine reglamentariamente, que no podrá contener datos de carácter personal sobre contratantes o investigados. El Ministerio del Interior y los órganos autonómicos competentes darán cuenta del funcionamiento del sector a las Cortes Generales y a los Parlamentos autonómicos correspondientes respectivamente, anualmente.

j) Depositar, en caso de cierre del despacho por cualquier causa, la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente.

2. Los titulares de despachos de detectives responderán civilmente de las acciones u omisiones en que, durante la ejecución de sus servicios, incurran los detectives privados dependientes o asociados.

TÍTULO III

Personal de seguridad privada

CAPÍTULO I

Disposiciones comunes

Artículo 26. *Profesiones de seguridad privada.*

1. Únicamente puede ejercer funciones de seguridad privada el personal de seguridad privada, que estará integrado por los vigilantes de seguridad y su especialidad de vigilantes de explosivos, los escoltas privados, los guardas rurales y sus especialidades de guardas de caza y guardapescas marítimos, los jefes de seguridad, los directores de seguridad y los detectives privados.

2. Para habilitarse como vigilante de explosivos será necesario haber obtenido previamente la habilitación como vigilante de seguridad.

Para habilitarse como guarda de caza o guardapesca marítimo será necesario haberlo hecho previamente como guarda rural.

3. Para la prestación de servicios en infraestructuras críticas y en aquéllos que tengan el carácter de esenciales para la comunidad, así como en aquéllos otros que excepcionalmente lo requieran en función de sus características específicas, se podrá incrementar reglamentariamente la exigencia formativa al personal de seguridad privada encargado de su realización.

4. Reglamentariamente se regulará la obtención por el personal de seguridad privada de habilitaciones adicionales a las ya adquiridas. El desarrollo reglamentario contemplará la exclusión de los requisitos de formación ya acreditados y valorará para la adquisición de dicha habilitación adicional la experiencia acreditada en el desarrollo de funciones de seguridad privada.

5. La uniformidad, distintivos y medios de defensa de los vigilantes de seguridad y de los guardas rurales y sus respectivas especialidades se determinarán reglamentariamente.

Artículo 27. *Habilitación profesional.*

1. Para el ejercicio de las funciones de seguridad privada, el personal al que se refiere el artículo anterior habrá de obtener previamente la correspondiente habilitación del Ministerio del Interior, en los términos que reglamentariamente se determinen.

2. A quienes soliciten la habilitación, previa comprobación de que reúnen los requisitos necesarios, se les expedirá la tarjeta de identidad profesional, que incluirá todas las habilitaciones de las que el titular disponga.

La tarjeta de identidad profesional constituirá el documento público de acreditación del personal de seguridad privada mientras se encuentra en el ejercicio de sus funciones profesionales.

3. La habilitación de todo el personal de seguridad privada corresponderá a la Dirección General de la Policía, excepto la de los guardas rurales y sus especialidades que corresponderá a la Dirección General de la Guardia Civil.

4. El personal de seguridad privada ejercerá exclusivamente las funciones para los que se encuentre habilitado.

5. Reglamentariamente se determinará el régimen de incompatibilidades para el ejercicio de funciones de seguridad privada.

Artículo 28. *Requisitos generales.*

1. Para la obtención de las habilitaciones profesionales indicadas en el artículo anterior, los aspirantes habrán de reunir, los siguientes requisitos generales:

a) Tener la nacionalidad de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo, o ser nacional de un

tercer Estado que tenga suscrito con España un convenio internacional en el que cada parte reconozca el acceso al ejercicio de estas actividades a los nacionales de la otra.

b) Ser mayor de edad.

c) Poseer la capacidad física y la aptitud psicológica necesarias para el ejercicio de las funciones.

d) Estar en posesión de la formación previa requerida en el artículo 29.

e) Carecer de antecedentes penales por delitos dolosos.

f) No haber sido sancionado en los dos o cuatro años anteriores por infracción grave o muy grave, respectivamente, en materia de seguridad privada.

g) No haber sido separado del servicio en las Fuerzas y Cuerpos de Seguridad o en las Fuerzas Armadas españolas o del país de su nacionalidad o procedencia en los dos años anteriores.

h) No haber sido condenado por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud.

i) Superar, en su caso, las pruebas de comprobación que reglamentariamente establezca el Ministerio del Interior, que acrediten los conocimientos y la capacidad necesarios para el ejercicio de sus funciones.

2. Además de los requisitos generales establecidos en el apartado anterior, el personal de seguridad privada habrá de reunir, para su habilitación, los requisitos específicos que reglamentariamente se determinen en atención a las funciones que haya de desempeñar.

3. La pérdida de alguno de los requisitos establecidos en este artículo producirá la extinción de la habilitación y la cancelación de oficio de la inscripción en el Registro Nacional.

4. Podrán habilitarse, pero no podrán ejercer funciones propias del personal de seguridad privada, los funcionarios públicos en activo y demás personal al servicio de cualquiera de las administraciones públicas, excepto cuando desempeñen la función de director de seguridad en el propio centro a que pertenezcan.

Los miembros de las Fuerzas y Cuerpos de Seguridad podrán ejercer funciones propias del personal de seguridad privada cuando pasen a una situación administrativa distinta a la de servicio activo, siempre que en los dos años anteriores no hayan desempeñado funciones de control de las entidades, servicios o actuaciones de seguridad, vigilancia o investigación privadas, ni de su personal o medios.

5. Los nacionales de otros Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, cuya habilitación o cualificación profesional haya sido obtenida en alguno de dichos Estados para el desempeño de funciones de seguridad privada en el mismo, podrán prestar servicios en España, siempre que, previa comprobación por el Ministerio del Interior, se acredite que cumplen los siguientes requisitos:

a) Poseer alguna titulación, habilitación o certificación expedida por las autoridades competentes de cualquier Estado miembro o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo que les autorice para el ejercicio de funciones de seguridad privada en el mismo.

b) Acreditar los conocimientos, formación y aptitudes equivalentes a los exigidos en España para el ejercicio de las profesiones relacionadas con la seguridad privada.

c) Tener conocimientos de lengua castellana suficientes para el normal desempeño de las funciones de seguridad privada.

d) Los previstos en los párrafos b), e), f), g) y h) del apartado 1.

6. La carencia o insuficiencia de conocimientos o aptitudes necesarios para el ejercicio en España de funciones de seguridad privada por parte de los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, podrá suplirse por aplicación de las medidas compensatorias previstas en la normativa vigente sobre reconocimiento de cualificaciones profesionales, de conformidad con lo que se determine reglamentariamente.

Artículo 29. *Formación.*

1. La formación requerida para el personal de seguridad privada consistirá:

a) Para los vigilantes de seguridad, vigilantes de explosivos, escoltas privados, guardas rurales, guardas de caza y guardapescas marítimos, en la obtención de la certificación acreditativa correspondiente, expedida por un centro de formación de personal de seguridad privada que haya presentado la declaración responsable ante el Ministerio del Interior o el órgano autonómico competente, o de los correspondientes certificados de profesionalidad de vigilancia y seguridad privada y guarderío rural y marítimo, que establezca el Gobierno a propuesta del Ministerio de Empleo y Seguridad Social, o del título de formación profesional que establezca el Gobierno a propuesta del Ministerio de Educación, Cultura y Deporte. En estos dos últimos casos no se exigirá la prueba de comprobación de conocimientos y capacidad a que se refiere el artículo 28.1.i).

b) Para los jefes y directores de seguridad, en la obtención bien de un título universitario oficial de grado en el ámbito de la seguridad que acredite la adquisición de las competencias que se determinen, o bien del título del curso de dirección de seguridad, reconocido por el Ministerio del Interior.

c) Para los detectives privados, en la obtención bien de un título universitario de grado en el ámbito de la investigación privada que acredite la adquisición de las competencias que se determinen, o bien del título del curso de investigación privada, reconocido por el Ministerio del Interior.

2. Cuando se trate de miembros de las Fuerzas y Cuerpos de Seguridad y de las Fuerzas Armadas se tendrá en cuenta, en la forma que reglamentariamente se establezca, el grado y experiencia profesionales que acrediten su cualificación para el desempeño de las diferentes funciones de seguridad privada, siendo exigible en todo caso la prueba de comprobación de conocimientos y capacidad a que se refiere el artículo 28.1.i).

3. En relación con lo dispuesto en el apartado 1, la formación previa del personal comprendido en su párrafo a) que no posea la titulación correspondiente de formación profesional, o los certificados de profesionalidad, así como su actualización y especialización se llevará a cabo en los centros de formación de seguridad privada que hayan presentado la declaración responsable ante el Ministerio del Interior o el órgano autonómico competente. y por profesores acreditados por el citado Ministerio.

4. Los centros de formación del personal de seguridad privada requerirán, para su apertura y funcionamiento, de la presentación de la correspondiente declaración responsable ante el Ministerio del Interior u órgano autonómico competente, debiendo reunir, entre otros que reglamentariamente se establezcan, los siguientes requisitos:

a) Acreditación, por cualquier título, del derecho de uso del inmueble.
b) Licencia municipal correspondiente.
c) Relación de profesores acreditados.
d) Instalaciones adecuadas al cumplimiento de sus fines.

5. No podrán ser titulares ni desempeñar funciones de dirección ni de administración de centros de formación del personal de seguridad privada los miembros de las Fuerzas y Cuerpos de Seguridad que hayan ejercido en los mismos funciones de control de las entidades, servicios o actuaciones, o del personal o medios, en materia de seguridad privada en los dos años anteriores.

6. Las empresas de seguridad privada podrán crear centros de formación y actualización para personal de seguridad privada perteneciente o no a sus plantillas, en los términos previstos en el apartado 4.

7. El Ministerio del Interior elaborará los programas de formación previa y especializada correspondiente al personal de seguridad privada, en cuyo contenido se incluirán materias específicas de respeto a la diversidad y a la igualdad de trato y no discriminación.

Artículo 30. *Principios de actuación.*

Además de lo establecido en el artículo 8, el personal de seguridad privada se atendrá en sus actuaciones a los siguientes principios básicos:

a) Legalidad.
b) Integridad.
c) Dignidad en el ejercicio de sus funciones.
d) Corrección en el trato con los ciudadanos.
e) Congruencia, aplicando medidas de seguridad y de investigación proporcionadas y adecuadas a los riesgos.
f) Proporcionalidad en el uso de las técnicas y medios de defensa y de investigación.
g) Reserva profesional sobre los hechos que conozca en el ejercicio de sus funciones.
h) Colaboración con las Fuerzas y Cuerpos de Seguridad. El personal de seguridad privada estará obligado a auxiliar y colaborar especialmente con las Fuerzas y Cuerpos de Seguridad, a facilitarles la información que resulte necesaria para el ejercicio de sus funciones, y a seguir sus instrucciones en relación con el servicio de seguridad privada que estuvieren prestando.

Artículo 31. *Protección jurídica de agente de la autoridad.*

Se considerarán agresiones y desobediencias a agentes de la autoridad las que se cometan contra el personal de seguridad privada, debidamente identificado, cuando desarrolle actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad.

CAPÍTULO II

Funciones de seguridad privada

Artículo 32. *Vigilantes de seguridad y su especialidad.*

1. Los vigilantes de seguridad desempeñarán las siguientes funciones:

a) Ejercer la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto privados como públicos, así como la protección de las personas que puedan encontrarse en los mismos, llevando a cabo las comprobaciones, registros y prevenciones necesarias para el cumplimiento de su misión.
b) Efectuar controles de identidad, de objetos personales, paquetería, mercancías o vehículos, incluido el interior de éstos, en el acceso o en el interior de inmuebles o propiedades donde presten servicio, sin que, en ningún caso, puedan retener la documentación personal, pero sí impedir el acceso a dichos inmuebles o propiedades. La negativa a exhibir la identificación o a permitir el control de los objetos personales, de paquetería, mercancía o del vehículo facultará para impedir a los particulares el acceso o para ordenarles el abandono del inmueble o propiedad objeto de su protección.
c) Evitar la comisión de actos delictivos o infracciones administrativas en relación con el objeto de su protección, realizando las comprobaciones necesarias para prevenirlos o impedir su consumación, debiendo oponerse a los mismos e intervenir cuando presenciaren la comisión de algún tipo de infracción o fuere precisa su ayuda por razones humanitarias o de urgencia.
d) En relación con el objeto de su protección o de su actuación, detener y poner inmediatamente a disposición de las Fuerzas y Cuerpos de Seguridad competentes a los delincuentes y los instrumentos, efectos y pruebas de los delitos, así como denunciar a quienes cometan infracciones administrativas. No podrán proceder al interrogatorio de aquéllos, si bien no se considerará como tal la anotación de sus datos personales para su comunicación a las autoridades.
Lo dispuesto en el párrafo anterior se entiende sin perjuicio de los supuestos en los que la Ley de Enjuiciamiento Criminal permite a cualquier persona practicar la detención.
e) Proteger el almacenamiento, recuento, clasificación, transporte y dispensado de dinero, obras de arte y antigüedades, valores y otros objetos valiosos, así como el manipulado de efectivo y demás procesos inherentes a la ejecución de estos servicios.
f) Llevar a cabo, en relación con el funcionamiento de centrales receptoras de alarmas, la prestación de servicios de verificación personal y respuesta de las señales de alarmas que se produzcan.

Además, también podrán realizar las funciones de recepción, verificación no personal y transmisión a las Fuerzas y Cuerpos de Seguridad que el artículo 47.1 reconoce a los operadores de seguridad.

2. Los vigilantes de seguridad se dedicarán exclusivamente a las funciones de seguridad propias, no pudiendo simultanearlas con otras no directamente relacionadas con aquéllas.

3. Corresponde a los vigilantes de explosivos, que deberán estar integrados en empresas de seguridad, la función de protección del almacenamiento, transporte y demás procesos inherentes a la ejecución de estos servicios, en relación con explosivos u otros objetos o sustancias peligrosas que reglamentariamente se determinen.

Será aplicable a los vigilantes de explosivos lo establecido para los vigilantes de seguridad respecto a uniformidad, armamento y prestación del servicio.

Artículo 33. *Escoltas privados.*

1. Son funciones de los escoltas privados el acompañamiento, defensa y protección de personas determinadas, o de grupos concretos de personas, impidiendo que sean objeto de agresiones o actos delictivos.

2. En el desempeño de sus funciones, los escoltas no podrán realizar identificaciones o detenciones, ni impedir o restringir la libre circulación, salvo que resultare imprescindible como consecuencia de una agresión o de un intento manifiesto de agresión a la persona o personas protegidas o a los propios escoltas, debiendo, en tal caso, poner inmediatamente al detenido o detenidos a disposición de las Fuerzas y Cuerpos de Seguridad, sin proceder a ninguna suerte de interrogatorio.

3. Para el cumplimiento de las indicadas funciones será aplicable a los escoltas privados lo determinado en el artículo 32 y demás preceptos concordantes, relativos a vigilantes de seguridad, salvo lo referente a la uniformidad.

Artículo 34. *Guardas rurales y sus especialidades.*

1. Los guardas rurales ejercerán funciones de vigilancia y protección de personas y bienes en fincas rústicas, así como en las instalaciones agrícolas, industriales o comerciales que se encuentren en ellas.

Se atendrán al régimen general establecido para los vigilantes de seguridad, con la especificidad de que no podrán desempeñar las funciones contempladas en el artículo 32.1.e).

2. A los guardas de caza corresponde desempeñar las funciones previstas en el apartado anterior para los guardas rurales y, además, las de vigilancia y protección en las fincas de caza en cuanto a los distintos aspectos del régimen cinegético y espacios de pesca fluvial.

3. Corresponde a los guardapescas marítimos desempeñar las funciones previstas en el apartado 1 para los guardas rurales y, además, las de vigilancia y protección de los establecimientos de acuicultura y zonas marítimas con fines pesqueros.

4. Los guardas de caza y los guardapescas marítimos podrán proceder a la retirada u ocupación de las piezas cobradas y los medios de caza y pesca, incluidas armas, cuando aquéllos hubieran sido utilizados para cometer una infracción, procediendo a su entrega inmediata a las Fuerzas y Cuerpos de Seguridad competentes.

Artículo 35. *Jefes de seguridad.*

1. En el ámbito de la empresa de seguridad en cuya plantilla están integrados, corresponde a los jefes de seguridad el ejercicio de las siguientes funciones:

a) El análisis de situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implantación y realización de los servicios de seguridad privada.

b) La organización, dirección e inspección del personal y servicios de seguridad privada.

c) La propuesta de los sistemas de seguridad que resulten pertinentes, y el control de su funcionamiento y mantenimiento, pudiendo validarlos provisionalmente hasta tanto se produzca la inspección y autorización, en su caso, por parte de la Administración.

d) El control de la formación permanente del personal de seguridad que de ellos dependa, y la propuesta de la adopción de las medidas o iniciativas adecuadas para el cumplimiento de dicha finalidad.

e) La coordinación de los distintos servicios de seguridad que de ellos dependan, con actuaciones propias de protección civil en situaciones de emergencia, catástrofe o calamidad pública.

f) La garantía de la colaboración de los servicios de seguridad con los de las correspondientes dependencias de las Fuerzas y Cuerpos de Seguridad.

g) La supervisión de la observancia de la normativa de seguridad privada aplicable.

h) La responsabilidad sobre la custodia y el traslado de armas de titularidad de la empresa a la que pertenezca, de acuerdo con la normativa de armas y con lo que reglamentariamente se determine.

2. La existencia del jefe de seguridad en las empresas de seguridad privada será obligatoria siempre que éstas se dediquen a todas o algunas de las actividades previstas en los párrafos a), b), c), d) y e) del artículo 5.1.

En función de la complejidad organizativa o técnica, u otras circunstancias que se determinen reglamentariamente, podrá exigirse la existencia de un jefe de seguridad específico para algunas de dichas actividades de seguridad.

3. El ejercicio de funciones podrá delegarse por los jefes de seguridad en los términos que reglamentariamente se dispongan.

Artículo 36. *Directores de seguridad.*

1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de seguridad el ejercicio de las siguientes funciones:

a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.

b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.

c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.

d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.

e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.

f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.

g) La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.

h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.

i) Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial.

2. Los usuarios de seguridad privada situarán al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad cuando así lo exija la normativa de desarrollo de esta ley por la dimensión de su servicio de seguridad; cuando se acuerde por decisión gubernativa, en atención a las medidas de seguridad y al grado de concentración de riesgo, o cuando lo prevea una disposición especial.

Lo dispuesto en este apartado es igualmente aplicable a las empresas de seguridad privada.

3. En las empresas de seguridad el director de seguridad podrá compatibilizar sus funciones con las de jefe de seguridad.

4. Cuando una empresa de seguridad preste servicio a un usuario que cuente con su propio director de seguridad, las funciones encomendadas a los jefes de seguridad en el artículo 35.1.a), b), c), y e) serán asumidas por dicho director de seguridad.

5. El ejercicio de funciones podrá delegarse por los directores de seguridad en los términos que reglamentariamente se disponga.

Artículo 37. *Detectives privados.*

1. Los detectives privados se encargarán de la ejecución personal de los servicios de investigación privada a los que se refiere el artículo 48, mediante la realización de averiguaciones en relación con personas, hechos y conductas privadas.

2. En el ejercicio de sus funciones, los detectives privados vendrán obligados a:

a) Confeccionar los informes de investigación relativos a los asuntos que tuvieren encargados.

b) Asegurar la necesaria colaboración con las Fuerzas y Cuerpos de Seguridad cuando sus actuaciones profesionales se encuentren relacionadas con hechos delictivos o que puedan afectar a la seguridad ciudadana.

c) Ratificar el contenido de sus informes de investigación ante las autoridades judiciales o policiales cuando fueren requeridos para ello.

3. El ejercicio de las funciones correspondientes a los detectives privados no será compatible con las funciones del resto del personal de seguridad privada, ni con funciones propias del personal al servicio de cualquier Administración Pública.

4. Los detectives privados no podrán investigar delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento.

TÍTULO IV

Servicios y medidas de seguridad

CAPÍTULO I

Disposiciones comunes

Artículo 38. *Prestación de los servicios de seguridad privada.*

1. Los servicios de seguridad privada se prestarán de conformidad con lo dispuesto en esta ley, en particular en sus artículos 8 y 30, y en sus normas de desarrollo, con arreglo a las estipulaciones del contrato, así como, en su caso, con la autorización concedida o declaración responsable presentada.

2. Los servicios de seguridad privada se prestarán únicamente por empresas de seguridad privada, despachos de detectives y personal de seguridad privada.

3. Reglamentariamente se establecerán las condiciones y requisitos para la subcontratación de servicios de seguridad privada.

4. Los vigilantes de seguridad, vigilantes de explosivos, escoltas privados y jefes de seguridad desempeñarán sus funciones profesionales integrados en las empresas de seguridad que les tengan contratados.

5. Los directores de seguridad de las empresas de seguridad privada y de las entidades obligadas a disponer de esta figura, conforme a lo dispuesto en el artículo 36, desempeñarán sus funciones integrados en las plantillas de dichas empresas.

6. Los guardas rurales podrán desarrollar sus funciones sin necesidad de constituir o estar integrados en empresas de seguridad, prestando sus servicios directamente a los titulares de bienes y derechos que les puedan contratar, conforme a lo que se establezca reglamentariamente, cuando se trate de servicios de vigilancia y protección de explotaciones

agrícolas, fincas de caza, en cuanto a los distintos aspectos del régimen cinegético, y zonas marítimas protegidas con fines pesqueros.

7. Los detectives privados ejercerán sus funciones profesionales a través de los despachos de detectives para los que presten sus servicios.

Artículo 39. *Forma de prestación.*

1. Los medios utilizados por las empresas de seguridad en la prestación de los servicios de seguridad privada deberán estar homologados por el Ministerio del Interior. En todo caso, los vehículos, uniformes y distintivos no podrán inducir a confusión con los de las Fuerzas y Cuerpos de Seguridad, ni con los de las Fuerzas Armadas, y se ajustarán a las características que reglamentariamente se determinen.

2. El personal de seguridad privada uniformado, constituido por los vigilantes de seguridad y de explosivos y por los guardas rurales y sus especialidades, prestará sus servicios vistiendo el uniforme y ostentando el distintivo del cargo, y portando los medios de defensa reglamentarios, que no incluirán armas de fuego.

Reglamentariamente se podrán establecer excepciones a la obligación de desarrollar sus funciones con uniforme y distintivo.

3. Previo el otorgamiento de las correspondientes licencias, sólo se desarrollarán con armas de fuego los servicios de seguridad privada contemplados en el artículo 40 y los que reglamentariamente se determinen.

Las armas adecuadas para realizar los servicios de seguridad sólo se podrán portar estando de servicio, con las salvedades que se establezcan reglamentariamente.

4. Salvo en los casos expresamente previstos en esta ley y lo que se determine reglamentariamente atendiendo a las especiales características de determinados servicios de seguridad privada, los vigilantes de seguridad ejercerán sus funciones en el interior de los inmuebles o de las propiedades de cuya vigilancia estuvieran encargados.

5. El personal de seguridad privada, durante la prestación de los servicios de seguridad privada, portará la tarjeta de identidad profesional y, en su caso, la documentación correspondiente al arma de fuego.

CAPÍTULO II

Servicios de las empresas de seguridad privada

Artículo 40. *Servicios con armas de fuego.*

1. Los siguientes servicios de seguridad privada se prestarán con armas de fuego en los términos que reglamentariamente se determinen:

a) Los de vigilancia y protección del almacenamiento, recuento, clasificación y transporte de dinero, valores y objetos valiosos.

b) Los de vigilancia y protección de fábricas y depósitos o transporte de armas, cartuchería metálica y explosivos.

c) Los de vigilancia y protección en buques mercantes y buques pesqueros que naveguen bajo bandera española en aguas en las que exista grave riesgo para la seguridad de las personas o de los bienes.

d) Cuando por sus características y circunstancias lo requieran, los de vigilancia y protección perimetral en centros penitenciarios, centros de internamiento de extranjeros, establecimientos militares u otros edificios o instalaciones de organismos públicos, incluidas las infraestructuras críticas.

2. Reglamentariamente se determinarán aquellos supuestos en los que, valoradas circunstancias tales como localización, valor de los objetos a proteger, concentración del riesgo, peligrosidad, nocturnidad, zonas rústicas o cinegéticas, u otras de análoga significación, podrá autorizarse la prestación de los servicios de seguridad privada portando armas de fuego.

Asimismo, podrá autorizarse la prestación de los servicios de verificación personal de alarmas portando armas de fuego, cuando sea necesario para garantizar la seguridad del

personal que los presta, atendiendo a la naturaleza de dicho servicio, al objeto de la protección o a otras circunstancias que incidan en aquélla.

3. El personal de seguridad privada sólo podrá portar el arma de fuego cuando esté de servicio, y podrá acceder con ella al lugar donde se desarrolle éste, salvo que legalmente se establezca lo contrario. Reglamentariamente podrán establecerse excepciones para supuestos determinados.

4. Las armas de fuego adecuadas para realizar cada tipo de servicio serán las que reglamentariamente se establezcan.

Artículo 41. *Servicios de vigilancia y protección.*

1. Los servicios de vigilancia y protección referidos a las actividades contempladas en el artículo 5.1.a) se prestarán por vigilantes de seguridad o, en su caso, por guardas rurales, que desempeñarán sus funciones, con carácter general, en el interior de los edificios, de las instalaciones o propiedades a proteger. No obstante, podrán prestarse fuera de estos espacios sin necesidad de autorización previa, incluso en vías o espacios públicos o de uso común, en los siguientes supuestos:

a) La vigilancia y protección sobre acciones de manipulación o utilización de bienes, maquinaria o equipos valiosos que hayan de tener lugar en las vías o espacios públicos o de uso común.

b) La retirada y reposición de fondos en cajeros automáticos, así como la prestación de servicios de vigilancia y protección de los mismos durante las citadas operaciones, o en las de reparación de averías.

c) Los desplazamientos al exterior de los inmuebles objeto de protección para la realización de actividades directamente relacionadas con las funciones de vigilancia y seguridad de dichos inmuebles.

d) La vigilancia y protección de los medios de transporte y de sus infraestructuras.

e) Los servicios de ronda o de vigilancia discontinua, consistentes en la visita intermitente y programada a los diferentes puestos de vigilancia establecidos o a los distintos lugares objeto de protección.

f) La persecución de quienes sean sorprendidos en flagrante delito, en relación con las personas o bienes objeto de su vigilancia y protección.

g) Las situaciones en que ello viniera exigido por razones humanitarias.

h) Los servicios de vigilancia y protección a los que se refieren los apartados siguientes.

2. Requerirán autorización previa por parte del órgano competente los siguientes servicios de vigilancia y protección, que se prestarán en coordinación, cuando proceda, con las Fuerzas y Cuerpos de Seguridad, y de acuerdo con sus instrucciones:

a) La vigilancia en polígonos industriales y urbanizaciones delimitados, incluidas sus vías o espacios de uso común.

b) La vigilancia en complejos o parques comerciales y de ocio que se encuentren delimitados.

c) La vigilancia en acontecimientos culturales, deportivos o cualquier otro evento de relevancia social que se desarrolle en vías o espacios públicos o de uso común, en coordinación, en todo caso, con las Fuerzas y Cuerpos de Seguridad.

d) La vigilancia y protección en recintos y espacios abiertos que se encuentren delimitados.

Reglamentariamente se establecerán las condiciones y requisitos para la prestación de estos servicios.

3. Cuando así se decida por el órgano competente, y cumpliendo estrictamente las órdenes e instrucciones de las Fuerzas y Cuerpos de Seguridad, podrán prestarse los siguientes servicios de vigilancia y protección:

a) La vigilancia perimetral de centros penitenciarios.

b) La vigilancia perimetral de centros de internamiento de extranjeros.

c) La vigilancia de otros edificios o instalaciones de organismos públicos.

d) La participación en la prestación de servicios encomendados a la seguridad pública, complementando la acción policial. La prestación de estos servicios también podrá realizarse por guardas rurales.

Artículo 42. *Servicios de videovigilancia.*

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

Artículo 43. *Servicios de protección personal.*

1. Los servicios de protección personal, a cargo de escoltas privados, consistirán en el acompañamiento, custodia, resguardo, defensa y protección de la libertad, vida e integridad física de personas o grupos de personas determinadas.

2. La prestación de servicios de protección personal se realizará con independencia del lugar donde se encuentre la persona protegida, incluido su tránsito o circulación por las vías públicas, sin que se puedan realizar identificaciones, restricciones de la circulación, o detenciones, salvo en caso de flagrante delito relacionado con el objeto de su protección.

3. La prestación de estos servicios sólo podrá realizarse previa autorización del Ministerio del Interior o del órgano autonómico competente, conforme se disponga reglamentariamente.

Artículo 44. *Servicios de depósito de seguridad.*

1. Los servicios de depósito de seguridad, referidos a la actividad contemplada en el artículo 5.1.c), estarán a cargo de vigilantes de seguridad y se prestarán obligatoriamente cuando los objetos en cuestión alcancen las cuantías que reglamentariamente se

establezcan, así como cuando las autoridades competentes lo determinen en atención a los antecedentes y circunstancias relacionadas con dichos objetos.

2. Los servicios de depósito de seguridad referidos a la actividad contemplada en el artículo 5.1.d), estarán a cargo de vigilantes de explosivos y se prestarán obligatoriamente cuando precisen de vigilancia, cuidado y protección especial, de acuerdo con la normativa específica de cada materia o así lo dispongan las autoridades competentes en atención a los antecedentes y circunstancias relacionadas con dichos objetos o sustancias.

Artículo 45. *Servicios de transporte de seguridad.*

Los servicios de transporte y distribución de los objetos y sustancias a que se refiere el artículo anterior, se llevarán a cabo mediante vehículos acondicionados especialmente para cada tipo de transporte u otros elementos de seguridad específicos homologados para el transporte, y consistirán en su traslado material y su protección durante el mismo, por vigilantes de seguridad o vigilantes de explosivos, respectivamente, con arreglo a lo prevenido en esta ley y en sus normas reglamentarias de desarrollo.

Artículo 46. *Servicios de instalación y mantenimiento.*

1. Los servicios de instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad, previa elaboración, por ingenieros acreditados, del preceptivo proyecto de instalación, cuyas características se determinarán reglamentariamente.

2. Estos sistemas deberán someterse a revisiones preventivas con la periodicidad y forma que se determine reglamentariamente.

Artículo 47. *Servicios de gestión de alarmas.*

1. Los servicios de gestión de alarmas, a cargo de operadores de seguridad, consistirán en la recepción, verificación no personal y, en su caso, transmisión de las señales de alarma, relativas a la seguridad y protección de personas y bienes a las Fuerzas y Cuerpos de Seguridad competentes.

2. Los servicios de respuesta ante alarmas se prestarán por vigilantes de seguridad o, en su caso, por guardas rurales, y podrán comprender los siguientes servicios:

a) El depósito y custodia de las llaves de los inmuebles u objetos donde estén instalados los sistemas de seguridad conectados a la central de alarmas y, en su caso, su traslado hasta el lugar del que procediere la señal de alarma verificada o bien la apertura a distancia controlada desde la central de alarmas.

b) El desplazamiento de los vigilantes de seguridad o guardas rurales a fin de proceder a la verificación personal de la alarma recibida.

c) Facilitar el acceso a los servicios policiales o de emergencia cuando las circunstancias lo requieran, bien mediante aperturas remotas controladas desde la central de alarmas o con los medios y dispositivos de acceso de que se disponga.

3. Cuando los servicios se refirieran al análisis y monitorización de eventos de seguridad de la información y las comunicaciones, estarán sujetos a las especificaciones que reglamentariamente se determinen. Las señales de alarma referidas a estos eventos deberán ser puestas, cuando corresponda, en conocimiento del órgano competente, por el propio usuario o por la empresa con la que haya contratado la seguridad.

CAPÍTULO III

Servicios de los despachos de detectives privados

Artículo 48. *Servicios de investigación privada.*

1. Los servicios de investigación privada, a cargo de detectives privados, consistirán en la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos:

a) Los relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos.

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal.

2. La aceptación del encargo de estos servicios por los despachos de detectives privados requerirá, en todo caso, la acreditación, por el solicitante de los mismos, del interés legítimo alegado, de lo que se dejará constancia en el expediente de contratación e investigación que se abra.

3. En ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos.

4. En la prestación de los servicios de investigación, los detectives privados no podrán utilizar o hacer uso de medios, vehículos o distintivos que puedan confundirse con los de las Fuerzas y Cuerpos de Seguridad.

5. En todo caso, los despachos de detectives y los detectives privados encargados de las investigaciones velarán por los derechos de sus clientes con respeto a los de los sujetos investigados.

6. Los servicios de investigación privada se ejecutarán con respeto a los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.

Artículo 49. *Informes de investigación.*

1. Por cada servicio que les sea contratado, los despachos o los detectives privados encargados del asunto deberán elaborar un único informe en el que reflejarán el número de registro asignado al servicio, los datos de la persona que encarga y contrata el servicio, el objeto de la contratación, los medios, los resultados, los detectives intervinientes y las actuaciones realizadas, en las condiciones y plazos que reglamentariamente se establezcan.

2. En el informe de investigación únicamente se hará constar información directamente relacionada con el objeto y finalidad de la investigación contratada, sin incluir en él referencias, informaciones o datos que hayan podido averiguarse relativos al cliente o al sujeto investigado, en particular los de carácter personal especialmente protegidos, que no resulten necesarios o que no guarden directa relación con dicho objeto y finalidad ni con el interés legítimo alegado para la contratación.

3. Dicho informe estará a disposición del cliente, a quien se entregará, en su caso, al finalizar el servicio, así como a disposición de las autoridades policiales competentes para la inspección, en los términos previstos en el artículo 54.5.

4. Los informes de investigación deberán conservarse archivados, al menos, durante tres años, sin perjuicio de lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las imágenes y los sonidos

grabados durante las investigaciones se destruirán tres años después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador. En todo caso, el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal, especialmente sobre el bloqueo de datos previsto en la misma.

5. Las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador, conforme a lo dispuesto en el artículo 25.

Artículo 50. *Deber de reserva profesional.*

1. Los detectives privados están obligados a guardar reserva sobre las investigaciones que realicen, y no podrán facilitar datos o informaciones sobre éstas más que a las personas que se las encomendaron y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

2. Sólo mediante requerimiento judicial o solicitud policial relacionada con el ejercicio de sus funciones en el curso de una investigación criminal o de un procedimiento sancionador se podrá acceder al contenido de las investigaciones realizadas por los detectives privados.

CAPÍTULO IV

Medidas de seguridad privada

Artículo 51. *Adopción de medidas.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán dotarse de medidas de seguridad privada dirigidas a la protección de personas y bienes y al aseguramiento del normal desarrollo de sus actividades personales o empresariales.

2. Reglamentariamente, con la finalidad de prevenir la comisión de actos delictivos contra ellos o por generar riesgos directos para terceros o ser especialmente vulnerables, se determinarán los establecimientos e instalaciones industriales, comerciales y de servicios y los eventos que resulten obligados a adoptar medidas de seguridad, así como el tipo y características de las que deban implantar en cada caso.

3. El Ministerio del Interior o, en su caso, el órgano autonómico competente podrá ordenar que los titulares de establecimientos o instalaciones industriales, comerciales y de servicios y los organizadores de eventos adopten las medidas de seguridad que reglamentariamente se establezcan.

El órgano competente formulará la propuesta teniendo en cuenta, además de su finalidad preventiva de hechos delictivos y de evitación de riesgos, la naturaleza de la actividad, la localización de los establecimientos o instalaciones, la concentración de personas u otras circunstancias que la justifiquen y, previa audiencia del titular u organizador, resolverá motivadamente.

Cuando se considerase necesaria la implantación de dichas medidas en órganos u organismos públicos, el órgano competente formulará la correspondiente propuesta y, previo acuerdo con el órgano administrativo o entidad de los que dependan las instalaciones o locales necesitados de protección, dictará la resolución procedente.

4. Las sedes y delegaciones de las empresas de seguridad privada vinculadas a la operativa de seguridad y los despachos de detectives privados y sus sucursales estarán obligados a adoptar las medidas de seguridad que se establezcan reglamentariamente.

5. La celebración de eventos y la apertura o funcionamiento de establecimientos e instalaciones y de empresas de seguridad y sus delegaciones y despachos de detectives y sus sucursales, mencionados en los apartados 2 y 3, estará condicionada a la efectiva implantación de las medidas de seguridad que resulten obligatorias en cada caso.

6. Los órganos competentes podrán eximir de la implantación de medidas de seguridad obligatorias cuando las circunstancias que concurran en el caso concreto las hicieren innecesarias o improcedentes.

7. Los titulares de los establecimientos, instalaciones y empresas de seguridad privada y sus delegaciones, así como de los despachos de detectives privados y sus sucursales y los

organizadores de eventos, serán responsables de la adopción de las medidas de seguridad que resulten obligatorias en cada caso.

Las empresas de seguridad encargadas de la prestación de las medidas de seguridad que les sean contratadas, serán responsables de su correcta instalación, mantenimiento y funcionamiento, sin perjuicio de la responsabilidad en que puedan incurrir sus empleados o los titulares de los establecimientos, instalaciones u organizadores obligados, si cualquier anomalía en su funcionamiento les fuera imputable.

8. Quedarán sometidos a lo establecido en esta ley y en sus disposiciones de desarrollo los usuarios que, sin estar obligados, adopten medidas de seguridad, así como quienes adopten medidas de seguridad adicionales a las obligatorias, respecto de éstas.

Artículo 52. *Tipos de medidas.*

1. A los exclusivos efectos de esta ley, se podrán adoptar los siguientes tipos de medidas de seguridad, destinadas a la protección de personas y bienes:

a) De seguridad física, cuya funcionalidad consiste en impedir o dificultar el acceso a determinados lugares o bienes mediante la interposición de cualquier tipo de barreras físicas.

b) De seguridad electrónica, orientadas a detectar o advertir cualquier tipo de amenaza, peligro, presencia o intento de asalto o intrusión que pudiera producirse, mediante la activación de cualquier tipo de dispositivos electrónicos.

c) De seguridad informática, cuyo objeto es la protección y salvaguarda de la integridad, confidencialidad y disponibilidad de los sistemas de información y comunicación, y de la información en ellos contenida.

d) De seguridad organizativa, dirigidas a evitar o poner término a cualquier tipo de amenaza, peligro o ataque deliberado, mediante la disposición, programación o planificación de cometidos, funciones o tareas formalizadas o ejecutadas por personas; tales como la creación, existencia y funcionamiento de departamentos de seguridad o la elaboración y aplicación de todo tipo de planes de seguridad, así como cualesquiera otras de similar naturaleza que puedan adoptarse.

e) De seguridad personal, para la prestación de servicios de seguridad regulados en esta ley, distintos de los que constituyen el objeto específico de las anteriores.

2. Las características, elementos y finalidades de las medidas de seguridad de cualquier tipo, quien quiera que los utilice, se regularán reglamentariamente de acuerdo con lo previsto, en cuanto a sus grados y características, en las normas que contienen especificaciones técnicas para una actividad o producto. Asimismo dichas medidas de seguridad, medios materiales y sistemas de alarma deberán contar con la evaluación de los organismos de certificación acreditados en el momento de su instalación y tendrán vigencia indefinida, salvo deterioro o instalación de un nuevo sistema, que deberá ser conforme a la homologación que le resulte aplicable.

TÍTULO V

Control administrativo

Artículo 53. *Actuaciones de control.*

1. Corresponde a las Fuerzas y Cuerpos de Seguridad competentes en el ejercicio de las funciones de control de las empresas, despachos de detectives, de sus servicios o actuaciones y de su personal y medios en materia de seguridad privada, el cumplimiento de las órdenes e instrucciones que se impartan por los órganos a los que se refieren los artículos 12 y 13.

2. En el ejercicio de estas funciones, los miembros de las Fuerzas y Cuerpos de Seguridad competentes podrán requerir la información pertinente y adoptar las medidas provisionales que resulten necesarias, en los términos del artículo 55.

3. Cuando en el ejercicio de las actuaciones de control se detectase la posible comisión de una infracción administrativa, se instará a la autoridad competente para la incoación del

correspondiente procedimiento sancionador. Si se tratara de la posible comisión de un hecho delictivo, se pondrá inmediatamente en conocimiento de la autoridad judicial.

4. Toda persona que tuviera conocimiento de irregularidades cometidas en el ámbito de la seguridad privada podrá denunciarlas ante las autoridades o funcionarios competentes, a efectos del posible ejercicio de las actuaciones de control y sanción correspondientes.

5. El acceso por los órganos que tengan atribuida la competencia de control se limitará a los datos necesarios para la realización de la misma.

Artículo 54. *Actuaciones de inspección.*

1. Las Fuerzas y Cuerpos de Seguridad competentes establecerán planes anuales de inspección ordinaria sobre las empresas, los despachos de detectives privados, el personal, los servicios, los establecimientos, los centros de formación, las medidas de seguridad y cualesquiera otras actividades o servicios regulados en esta ley.

2. Al margen de los citados planes de inspección, cuando recibieren denuncias sobre irregularidades cometidas en el ámbito de la seguridad privada procederán a la comprobación de los hechos denunciados y, en su caso, a instar la incoación del correspondiente procedimiento sancionador.

3. A los efectos anteriormente indicados, las empresas de seguridad, los despachos de detectives y el personal de seguridad privada, así como los establecimientos obligados a contratar servicios de seguridad privada, los centros de formación, las centrales de alarma de uso propio y los usuarios que contraten dichos servicios, habrán de facilitar a las Fuerzas y Cuerpos de Seguridad competentes el acceso a sus instalaciones y medios a efectos de inspección, así como a la información contenida en los contratos de seguridad, en los informes de investigación y en los libros-registro, en los supuestos y en la forma que reglamentariamente se determine.

4. Las actuaciones de inspección se atendrán a los principios de injerencia mínima y proporcionalidad, y tendrán por finalidad la comprobación del cumplimiento de la legislación aplicable.

5. Cuando las actuaciones de inspección recaigan sobre los servicios de investigación privada se tendrá especial cuidado en su ejecución, extremándose las cautelas en relación con las imágenes, sonidos o datos personales obtenidos que obren en el expediente de investigación. Las actuaciones se limitarán a la comprobación de su existencia, sin entrar en su contenido, salvo que se encuentre relacionado con una investigación judicial o policial o con un expediente sancionador.

6. Las inspecciones a las que se refieren los apartados anteriores se realizarán por el Cuerpo Nacional de Policía; por la Guardia Civil, en el caso de los guardas rurales y sus especialidades y centros y cursos de formación relativos a este personal; o, por el cuerpo de policía autonómica competente.

7. Siempre que el personal indicado en el apartado anterior realice una inspección, extenderá el acta correspondiente y, en el caso de existencia de infracción, se dará cuenta a la autoridad competente.

8. El acceso por los órganos que tengan atribuida la competencia de inspección se limitará a los datos necesarios para la realización de la misma.

Artículo 55. *Medidas provisionales anteriores al procedimiento.*

1. Los miembros de las Fuerzas y Cuerpos de Seguridad competentes podrán acordar excepcionalmente las siguientes medidas provisionales anteriores a la eventual incoación de un procedimiento sancionador, dando cuenta de ello inmediatamente a la autoridad competente:

a) La ocupación o precinto de vehículos, armas, material o equipos prohibidos, no homologados o que resulten peligrosos o perjudiciales, así como de los instrumentos y efectos de la infracción, en supuestos de grave riesgo o peligro inminente para las personas o bienes.

b) La suspensión, junto con la intervención u ocupación de los medios o instrumentos que se estuvieren empleando, de aquellos servicios de seguridad que se estuvieren prestando sin las preceptivas garantías y formalidades legales o sin contar con la necesaria

autorización o declaración responsable, o cuando puedan causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana.

c) El cese de los servicios de seguridad cuando se constate que están siendo prestados por empresas, centrales de alarma de uso propio o despachos de detectives, no autorizados o que no hubieran presentado la declaración responsable, o por personal no habilitado o acreditado para el ejercicio legal de los mismos.

d) El cese de la actividad docente en materia de seguridad privada, cuando se constate que los centros que la imparten, no hayan presentado la declaración responsable o el profesorado no tuviera la acreditación correspondiente.

e) La desconexión de los sistemas de alarma cuyo mal funcionamiento causare perjuicios a la seguridad pública o molestias a terceros. Cuando se trate de establecimientos obligados a contar con esta medida de seguridad, la desconexión se suplirá mediante el establecimiento de un servicio permanente de vigilancia y protección privada.

f) La retirada de la tarjeta de identificación profesional al personal de seguridad o de la acreditación al personal acreditado, cuando resulten detenidos por su implicación en la comisión de hechos delictivos.

g) La suspensión, parcial o total, de las actividades de los establecimientos que sean notoriamente vulnerables y no tengan en funcionamiento las medidas de seguridad obligatorias.

2. Estas medidas habrán de ser ratificadas, modificadas o revocadas en el plazo máximo de quince días. En todo caso quedarán sin efecto si, transcurrido dicho plazo, no se incoa el procedimiento sancionador o el acuerdo de incoación no contiene un pronunciamiento expreso acerca de las mismas. El órgano competente para ratificar, revocar o modificar las medidas provisionales será el competente para incoar el procedimiento sancionador.

3. La duración de las medidas contempladas en el apartado 1, que deberá ser notificada a los interesados, no podrá exceder de seis meses.

4. Asimismo, con independencia de las responsabilidades penales o administrativas a que hubiere lugar, los miembros de las Fuerzas y Cuerpos de Seguridad competentes se harán cargo de las armas que se porten o utilicen ilegalmente, siguiendo lo dispuesto al respecto en la normativa de armas.

TÍTULO VI

Régimen sancionador

CAPÍTULO I

Infracciones

Artículo 56. *Clasificación y prescripción.*

1. Las infracciones de las normas contenidas en esta ley podrán ser leves, graves y muy graves.

2. Las infracciones leves prescribirán a los seis meses, las graves al año y las muy graves a los dos años.

3. El plazo de prescripción se contará desde la fecha en que la infracción hubiera sido cometida. En las infracciones derivadas de una actividad continuada, la fecha inicial del cómputo será la de la finalización de la actividad o la del último acto en que la infracción se consume.

4. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento sancionador, volviendo a correr el plazo si el expediente permaneciera paralizado durante seis meses por causa no imputable a aquellos contra quienes se dirija.

Artículo 57. *Infracciones de las empresas que desarrollen actividades de seguridad privada, de sus representantes legales, de los despachos de detectives privados y de las centrales de alarma de uso propio.*

Las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) La prestación de servicios de seguridad privada a terceros careciendo de autorización o, en su caso, sin haber presentado la declaración responsable prevista en el artículo 18.1 y 2 para la prestación de los servicios de que se trate.

b) La contratación o utilización, en servicios de seguridad privada, de personas que carezcan de la habilitación o acreditación correspondiente.

c) La realización de actividades prohibidas en el artículo 8.4, sobre reuniones o manifestaciones, conflictos políticos o laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad o investigación hubieran sido encargados, o cualquier otra forma de quebrantamiento del deber de reserva, cuando no sean constitutivas de delito y salvo que sean constitutivas de infracción a la normativa sobre protección de datos de carácter personal.

d) La instalación o utilización de medios materiales o técnicos no homologados cuando la homologación sea preceptiva y sean susceptibles de causar grave daño a las personas o a los intereses generales.

e) La negativa a facilitar, cuando proceda, la información contenida en los contratos de seguridad privada, en los libros-registro o el acceso a los informes de investigación privada.

f) El incumplimiento de las previsiones normativas sobre adquisición y uso de armas, así como sobre disponibilidad de armeros y custodia de aquéllas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por esta ley, o la contratación de instructores de tiro que carezcan de la oportuna habilitación.

g) La prestación de servicios de seguridad privada con armas de fuego fuera de lo dispuesto en esta ley.

h) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

i) El incumplimiento de la obligación que impone a los representantes legales el artículo 22.3.

j) La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegaciones y sucursales.

k) El incumplimiento de las condiciones de prestación de servicios establecidos por la autoridad competente en relación con el ejercicio del derecho de huelga en servicios esenciales, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

l) El incumplimiento de los requisitos que impone a las empresas de seguridad el artículo 19. 1, 2 y 3, y el artículo 35.2.

m) El incumplimiento de los requisitos que impone a los despachos de detectives el artículo 24. 1 y 2.

n) La falta de transmisión a las Fuerzas y Cuerpos de Seguridad competentes de las alarmas reales que se registren en las centrales receptoras de alarmas privadas, incluidas las de uso propio, así como el retraso en la transmisión de las mismas, cuando estas conductas no estén justificadas.

ñ) La prestación de servicios compatibles contemplados en el artículo 6.2, empleando personal no habilitado que utilice armas o medios de defensa reservados al personal de seguridad privada.

o) La realización de investigaciones privadas a favor de solicitantes en los que no concurra un interés legítimo en el asunto.

p) La prestación de servicios de seguridad privada sin formalizar los correspondientes contratos.

q) El empleo o utilización, en servicios de seguridad privada, de medidas o de medios personales, materiales o técnicos de forma que se atente contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, siempre que no constituyan delito.

r) La falta de comunicación por parte de empresas de seguridad informática de las incidencias relativas al sistema de cuya protección sean responsables cuando sea preceptivo.

s) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

t) La prestación de actividades ajenas a las de seguridad privada, excepto las compatibles previstas en el artículo 6 de la presente ley.

2. Infracciones graves:

a) La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

b) La prestación de servicios de seguridad privada con vehículos, uniformes, distintivos, armas o medios de defensa que no reúnan las características reglamentarias.

c) La prestación de servicios de seguridad privada careciendo de los requisitos específicos de autorización o presentación de declaración responsable para la realización de dicho tipo de servicios. Esta infracción también será aplicable cuando tales servicios se lleven a cabo fuera del lugar o del ámbito territorial para el que estén autorizados o se haya presentado la declaración responsable, o careciendo de la autorización previa o de dicha declaración cuando éstas sean preceptivas, o cuando se realicen en condiciones distintas a las expresamente previstas en la autorización del servicio.

d) La retención de la documentación profesional del personal de seguridad privada, o de la acreditación del personal acreditado.

e) La prestación de servicios de seguridad privada sin comunicar correctamente los correspondientes contratos al Ministerio del Interior o al órgano autonómico competente, o en los casos en que la comunicación se haya producido con posterioridad al inicio del servicio.

f) La prestación de servicios de seguridad privada sin cumplir lo estipulado en el correspondiente contrato.

g) La falta de sustitución ante el abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

h) La utilización, en el desempeño de funciones de seguridad privada, de personal de seguridad privada, con una antigüedad mínima de un año en la empresa, que no haya realizado los correspondientes cursos de actualización o especialización, no los haya superado, o no los haya realizado con la periodicidad que reglamentariamente se determine.

i) La falta de presentación al Ministerio del Interior o al órgano autonómico competente del certificado acreditativo de la vigencia del contrato de seguro, aval o seguro de caución en los términos establecidos en el artículo 19.1.e) y f) y 24.2.e) y f), así como la no presentación del informe de actividades y el resumen de la cuenta anual a los que se refiere el artículo 21.1.e), o la no presentación de la memoria a la que se refiere el artículo 25.1.i)

j) La comunicación de una o más falsas alarmas por negligencia, deficiente funcionamiento o falta de verificación previa.

k) La apertura de delegaciones o sucursales sin obtener la autorización necesaria o sin haber presentado la declaración responsable ante el órgano competente, cuando sea preceptivo.

l) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente, de las altas y bajas del personal de seguridad privada, así como de los cambios que se produzcan en sus representantes legales y toda variación en la composición personal de los órganos de administración, gestión, representación y dirección.

m) La prestación de servicio por parte del personal de seguridad privada sin la debida uniformidad o sin los medios que reglamentariamente sean exigibles.

n) La no realización de las revisiones anuales obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

ñ) La carencia o falta de cumplimentación de cualquiera de los libros-registro obligatorios.

o) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente de todo cambio relativo a su personalidad o forma jurídica, denominación, número de identificación fiscal o domicilio.

p) La falta de mantenimiento, en todo momento, de los requisitos establecidos para los representantes legales en el artículo 22.2.

q) El deficiente funcionamiento, por parte de las empresas de seguridad privada y despachos de detectives, en sus sedes, delegaciones o sucursales, de las medidas de seguridad obligatorias, así como el incumplimiento de las revisiones obligatorias de las mismas.

r) La prestación de servicios compatibles contemplados en el artículo 6.2 empleando personal no habilitado que utilice distintivos, uniformes o medios que puedan confundirse con los del personal de seguridad privada.

s) El incumplimiento de los requisitos impuestos a las empresas de seguridad informática.

t) La prestación de servicios incumpliendo lo dispuesto en el artículo 19.4.

u) La actuación de vigilantes de seguridad en el exterior de las instalaciones, inmuebles o propiedades de cuya vigilancia o protección estuvieran encargadas las empresas de seguridad privada con motivo de la prestación de servicios de tal naturaleza, fuera de los supuestos legalmente previstos.

v) No depositar la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente, en caso de cierre del despacho de detectives privados.

w) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

x) La publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

y) La prestación de servicios de seguridad privada en condiciones distintas a las previstas en las comunicaciones de los correspondientes contratos.

3. Infracciones leves:

a) El incumplimiento de la periodicidad de las revisiones obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

b) La utilización en los servicios de seguridad privada de vehículos, uniformes o distintivos con apariencia o semejanza a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

c) La falta de diligencia en la cumplimentación de los libros-registro obligatorios.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 58. *Infracciones del personal que desempeñe funciones de seguridad privada.*

El personal que desempeñe funciones de seguridad privada, así como los ingenieros, técnicos, operadores de seguridad y profesores acreditados, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) El ejercicio de funciones de seguridad privada para terceros careciendo de la habilitación o acreditación necesaria.

b) El incumplimiento de las previsiones contenidas en esta ley sobre tenencia de armas de fuego fuera del servicio y sobre su utilización.

c) La falta de reserva debida sobre los hechos que conozcan en el ejercicio de sus funciones o la utilización de medios materiales o técnicos de tal forma que atenten contra el

derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones cuando no constituyan delito.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

e) La negativa a identificarse profesionalmente, en el ejercicio de sus respectivas funciones, ante la Autoridad o sus agentes, cuando fueren requeridos para ello.

f) La realización de investigaciones sobre delitos perseguibles de oficio o la falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

g) La realización de actividades prohibidas en el artículo 8.4 sobre reuniones o manifestaciones, conflictos políticos y laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad estén encargados, en el caso de que no sean constitutivas de delito; salvo que sean constitutivas infracción a la normativa sobre protección de datos de carácter personal.

h) El ejercicio abusivo de sus funciones en relación con los ciudadanos.

i) La realización, orden o tolerancia, en el ejercicio de su actuación profesional, de prácticas abusivas, arbitrarias o discriminatorias, incluido el acoso, que entrañen violencia física o moral, cuando no constituyan delito.

j) El abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

k) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, sin disponer de la acreditación correspondiente expedida por el Ministerio del Interior.

l) La no realización del informe de investigación que preceptivamente deben elaborar los detectives privados o su no entrega al contratante del servicio, o la elaboración de informes paralelos.

m) El ejercicio de funciones de seguridad privada por parte del personal a que se refiere el artículo 28.3 y 4.

n) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

2. Infracciones graves:

a) La realización de funciones de seguridad privada que excedan de la habilitación obtenida.

b) El ejercicio de funciones de seguridad privada por personal habilitado, no integrado en empresas de seguridad privada, o en la plantilla de la empresa, cuando resulte preceptivo conforme a lo dispuesto en el artículo 38.5, o al margen de los despachos de detectives.

c) La falta de respeto al honor o a la dignidad de las personas.

d) El ejercicio del derecho a la huelga al margen de lo dispuesto al respecto para los servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

e) La no identificación profesional, en el ejercicio de sus respectivas funciones, cuando fueren requeridos para ello por los ciudadanos.

f) La retención de la documentación personal en contra de lo previsto en el artículo 32.1.b).

g) La falta de diligencia en el cumplimiento de las respectivas funciones por parte del personal habilitado o acreditado.

h) La identificación profesional haciendo uso de documentos o distintivos diferentes a los dispuestos legalmente para ello o acompañando éstos con emblemas o distintivos de apariencia semejante a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

i) La negativa a realizar los cursos de formación permanente a los que vienen obligados.

j) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, no ajustados a las normas técnicas reglamentariamente establecidas.

k) La omisión, total o parcial, de los datos que obligatoriamente debe contener el informe de investigación que deben elaborar los detectives privados.

l) El ejercicio de funciones de seguridad privada incompatibles entre sí, por parte de personal habilitado para ellas.

m) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

n) La validación provisional de sistemas o medidas de seguridad que no se adecuen a la normativa de seguridad privada.

3. Infracciones leves:

a) La actuación sin la debida uniformidad o medios, que reglamentariamente sean exigibles, o sin portar los distintivos o la documentación profesional, así como la correspondiente al arma de fuego utilizada en la prestación del servicio encomendado.

b) El trato incorrecto o desconsiderado con los ciudadanos.

c) La no cumplimentación, total o parcial, por parte de los técnicos acreditados, del documento justificativo de las revisiones obligatorias de los sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 59. *Infracciones de los usuarios y centros de formación.*

Los usuarios de servicios de seguridad privada y los centros de formación de personal de seguridad privada podrán incurrir en las siguientes infracciones:

1. Muy graves:

a) La contratación o utilización a sabiendas de los servicios de empresas de seguridad o despachos de detectives carentes de la autorización específica o declaración responsable necesaria para el desarrollo de los servicios de seguridad privada.

b) La utilización de aparatos de alarmas u otros dispositivos de seguridad no homologados cuando fueran susceptibles de causar grave daño a las personas o a los intereses generales.

c) El incumplimiento, por parte de los centros de formación, de los requisitos y condiciones exigidos en la declaración responsable, o impartir cursos sin haberla presentado.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad competentes en la realización de las funciones inspectoras de las medidas de seguridad, de los centros de formación y de los establecimientos obligados.

e) La no adecuación de los cursos que se impartan en los centros de formación a lo previsto reglamentariamente en cuanto a su duración, modalidades y contenido.

f) La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias.

g) La falta de comunicación de las incidencias detectadas y confirmadas en su centro de control de la seguridad de la información y las comunicaciones, cuando sea preceptivo.

h) La contratación o utilización a sabiendas de personas carentes de la habilitación o acreditación necesarias para la prestación de servicios de seguridad o la utilización de personal docente no acreditado en actividades de formación.

i) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

j) La entrada en funcionamiento, sin previa autorización, de centrales receptoras de alarmas de uso propio por parte de entidades públicas o privadas.

k) Obligar a personal habilitado contratado a realizar otras funciones distintas a aquellas para las que fue contratado.

2. Graves:

a) El incumplimiento de las revisiones preceptivas de los sistemas o medidas de seguridad obligatorias que tengan instalados.

b) La utilización de aparatos de alarma u otros dispositivos de seguridad no homologados.

c) La no comunicación al órgano competente de las modificaciones que afecten a cualquiera de los requisitos que dieron lugar a la autorización de los centros de formación.

d) La impartición de los cursos de formación fuera de las instalaciones autorizadas de los centros de formación.

e) El anormal funcionamiento de las medidas de seguridad obligatorias adoptadas o instaladas cuando ocasionen perjuicios a la seguridad pública o a terceros.

f) La utilización de personal docente no acreditado en actividades de formación.

g) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

h) El incumplimiento, por parte de los usuarios de seguridad privada, de la obligación de situar al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad, en contra de lo previsto en el artículo 36.2.

3. Leves:

a) La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen, o cuando su funcionamiento cause daños o molestias desproporcionados a terceros.

b) El anormal funcionamiento de las medidas o sistemas de seguridad que se tengan instalados.

c) Las irregularidades en la cumplimentación de los registros prevenidos.

d) En general, el incumplimiento de las obligaciones contenidas en esta ley que no constituya infracción grave o muy grave.

Artículo 60. *Colaboración reglamentaria.*

Las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones establecidas en esta ley que, sin constituir nuevas infracciones o sanciones, ni alterar la naturaleza o límites de las que en ella se contemplan, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las sanciones correspondientes.

CAPÍTULO II

Sanciones

Artículo 61. *Sanciones a las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 57, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 30.001 a 600.000 euros.

b) Extinción de la autorización, o cierre de la empresa o despacho en los casos de declaración responsable, que comportará la prohibición de volver a obtenerla o presentarla, respectivamente, por un plazo de entre uno y dos años, y cancelación de la inscripción en el registro correspondiente.

c) Prohibición para ocupar cargos de representación legal en empresas de seguridad privada por un plazo de entre uno y dos años.

2. Por la comisión de infracciones graves:

a) Multa de 3.001 a 30.000 euros.

b) Suspensión temporal de la autorización o de la declaración responsable por un plazo de entre seis meses y un año.

c) Prohibición para ocupar cargos de representación legal en empresas de seguridad privada por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 3.000 euros.

Artículo 62. *Sanciones al personal.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 58, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 6.001 a 30.000 euros.
b) Extinción de la habilitación, que comportará la prohibición de volver a obtenerla por un plazo de entre uno y dos años, y cancelación de la inscripción en el Registro Nacional.

2. Por la comisión de infracciones graves:

a) Multa de 1.001 a 6.000 euros.
b) Suspensión temporal de la habilitación por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 1.000 euros.

Artículo 63. *Sanciones a usuarios y centros de formación.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 59, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 20.001 a 100.000 euros.
b) Cierre del centro de formación, que comportará la prohibición de volver a presentar la declaración responsable para su apertura por un plazo de entre uno y dos años, y cancelación de la inscripción en el registro correspondiente.
c) La clausura, desde seis meses y un día a dos años, de los establecimientos que no tengan en funcionamiento las medidas de seguridad obligatorias.

2. Por la comisión de infracciones graves:

a) Multa de 3.001 a 20.000 euros.
b) Suspensión temporal de la declaración responsable del centro de formación por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 3.000 euros.

Artículo 64. *Graduación de las sanciones.*

Para la graduación de las sanciones, los órganos competentes tendrán en cuenta la gravedad y trascendencia del hecho, el posible perjuicio para el interés público, la situación de riesgo creada o mantenida para personas o bienes, la reincidencia, la intencionalidad, el volumen de actividad de la empresa de seguridad, despacho de detectives, centro de formación o establecimiento contra el que se dicte la resolución sancionadora, y la capacidad económica del infractor.

Artículo 65. *Aplicación de las sanciones.*

1. Las sanciones previstas en esta ley podrán aplicarse de forma alternativa o acumulativa.

2. La aplicación de sanciones pecuniarias tenderá a evitar que la comisión de las infracciones tipificadas no resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas.

Artículo 66. *Competencia sancionadora.*

1. En el ámbito de la Administración General del Estado, la potestad sancionadora corresponderá:

a) Al Ministro del Interior, para imponer las sanciones de extinción de las autorizaciones, habilitaciones y declaraciones responsables.

b) Al Secretario de Estado de Seguridad, para imponer las restantes sanciones por infracciones muy graves.

c) Al Director General de la Policía, para imponer las sanciones por infracciones graves.

Cuando, en el curso de las inspecciones por parte de la Guardia Civil de los cursos para guardas rurales, impartidos por centros de formación no exclusivos de éstos, se detecten posibles infracciones, la sanción corresponderá al Director General de la Policía.

d) Al Director General de la Guardia Civil, para imponer las sanciones por infracciones graves en relación con los guardas rurales y centros y cursos de formación exclusivos para este personal.

e) A los Delegados y a los Subdelegados del Gobierno, para imponer las sanciones por infracciones leves.

2. En el ámbito de las comunidades autónomas con competencia en materia de seguridad privada, la potestad sancionadora corresponderá a los titulares de los órganos que se determinen en cada caso.

3. Contra las resoluciones sancionadoras se podrán interponer los recursos previstos en la legislación de procedimiento administrativo y en la de la jurisdicción contencioso-administrativa.

Artículo 67. *Decomiso del material.*

El material prohibido, no homologado o indebidamente utilizado en servicios de seguridad privada, será decomisado y se procederá a su destrucción si no fuera de lícito comercio, o a su enajenación en otro caso, quedando en depósito la cantidad que se obtuviera para hacer frente a las responsabilidades administrativas o de otro orden en que se haya podido incurrir.

Artículo 68. *Prescripción de las sanciones.*

1. Las sanciones impuestas por infracciones leves, graves o muy graves prescribirán, respectivamente, al año, a los dos años y a los cuatro años.

2. El plazo de prescripción comenzará a contarse desde el día siguiente a aquel en que sea firme la resolución por la que se impone la sanción, si ésta no se hubiese comenzado a ejecutar, o desde que se quebrantase el cumplimiento de la misma, si hubiese comenzado, y se interrumpirá desde que se comience o se reanude la ejecución o cumplimiento.

CAPÍTULO III

Procedimiento

Artículo 69. *Medidas cautelares.*

1. Iniciado el procedimiento sancionador, el órgano que haya ordenado su incoación podrá adoptar las medidas cautelares necesarias para garantizar su adecuada instrucción, así como para evitar la continuación de la infracción o asegurar el pago de la sanción, en el caso de que ésta fuese pecuniaria, y el cumplimiento de la misma en los demás supuestos.

2. Dichas medidas, que deberán ser congruentes con la naturaleza de la presunta infracción y proporcionadas a la gravedad de la misma, podrán consistir en:

a) La ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción.

b) La retirada preventiva de las autorizaciones, habilitaciones, permisos o licencias, o la suspensión, en su caso, de la eficacia de las declaraciones responsables.

c) La suspensión de la habilitación del personal de seguridad privada y, en su caso, de la tramitación del procedimiento para el otorgamiento de aquélla, mientras dure la instrucción de expedientes por infracciones graves o muy graves en materia de seguridad privada.

También podrán ser suspendidas las indicadas habilitación y tramitación, hasta tanto finalice el proceso por delitos contra dicho personal.

3. Las medidas cautelares previstas en los párrafos b) y c) del apartado anterior no podrán tener una duración superior a un año.

Artículo 70. *Ejecutoriedad.*

1. Las sanciones impuestas serán inmediatamente ejecutivas desde que la resolución adquiera firmeza en vía administrativa.

2. Cuando la sanción sea de naturaleza pecuniaria y no se haya previsto plazo para satisfacerla, la autoridad que la impuso lo señalará, sin que pueda ser inferior a quince ni superior a treinta días hábiles, pudiendo acordarse el fraccionamiento del pago.

3. En los casos de suspensión temporal y extinción de la eficacia de autorizaciones, habilitaciones o declaraciones responsables y prohibición del ejercicio de la representación legal de las empresas, la autoridad sancionadora señalará un plazo de ejecución suficiente, que no podrá ser inferior a quince días hábiles ni superior a dos meses, oyendo al sancionado y a los terceros que pudieran resultar directamente afectados.

Artículo 71. *Publicidad de las sanciones.*

Las sanciones, así como los nombres, apellidos, denominación o razón social de las personas físicas o jurídicas responsables de la comisión de infracciones muy graves, cuando hayan adquirido firmeza en vía administrativa, podrán ser hechas públicas, en virtud de acuerdo de la autoridad competente para su imposición, siempre que concurra riesgo para la seguridad de los usuarios o ciudadanos, reincidencia en infracciones de naturaleza análoga o acreditada intencionalidad.

Artículo 72. *Multas coercitivas.*

1. Para lograr el cumplimiento de las resoluciones sancionadoras, las autoridades competentes relacionadas en el artículo 66 podrán imponer multas coercitivas, de acuerdo con lo establecido en la legislación de procedimiento administrativo.

2. La cuantía de estas multas no excederá de 6.000 euros, pero podrá aumentarse sucesivamente en el 50 por 100 de la cantidad anterior en casos de reiteración del incumplimiento.

3. Las multas coercitivas serán independientes de las sanciones pecuniarias que puedan imponerse y compatibles con ellas.

Disposición adicional primera. *Comercialización de productos.*

En la comercialización de productos provenientes de los Estados miembros de la Unión Europea, del Espacio Económico Europeo o de cualquier tercer país con el que la Unión Europea tenga un acuerdo de asociación y que estén sometidos a reglamentaciones nacionales de seguridad, equivalentes a la reglamentación española de seguridad privada, se atenderá a los estándares previstos por las entidades de certificación acreditadas que ofrezcan, a través de su administración pública competente, garantías técnicas profesionales y de independencia e imparcialidad equivalentes a las exigidas por la legislación española, y a que las disposiciones del Estado, con base en las que se evalúa la conformidad, comporten un nivel de seguridad equivalente al exigido por las disposiciones legales aplicables.

Disposición adicional segunda. *Contratación de servicios de seguridad privada por las administraciones públicas.*

1. En consideración a la relevancia para la seguridad pública de los servicios de seguridad privada, de conformidad con el artículo 118 del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, los órganos de contratación de las administraciones públicas podrán establecer condiciones especiales de ejecución de los contratos de servicios de seguridad relacionadas con el cumplimiento de las obligaciones laborales por parte de las empresas de seguridad privada contratistas.

2. Los pliegos de cláusulas administrativas particulares o los contratos podrán establecer penalidades para el caso de incumplimiento de estas condiciones especiales de ejecución, o atribuirles el carácter de obligaciones contractuales esenciales a los efectos de la resolución de los contratos, de acuerdo con los artículos 212.1 y 223.f).

Disposición adicional tercera. *Cooperación administrativa.*

En consideración a la relevancia para la seguridad pública de los servicios de seguridad privada, los órganos competentes en materia policial, tributaria, laboral y de seguridad social establecerán mecanismos de información, control e inspección conjunta en relación con las empresas de seguridad privada para evitar el fraude y el intrusismo.

Disposición transitoria primera. *Habilitaciones profesionales anteriores a la entrada en vigor de esta ley.*

1. Las habilitaciones del personal de seguridad privada obtenidas antes de la entrada en vigor de esta ley mantendrán su validez sin necesidad de convalidación o canje alguno.

2. Las habilitaciones correspondientes a los guardas particulares del campo se entenderán hechas a la nueva categoría de guardas rurales.

Disposición transitoria segunda. *Personal de centrales receptoras de alarmas.*

Quienes a la entrada en vigor de esta ley estuvieran desempeñando su actividad en centrales receptoras de alarmas, podrán continuar desarrollando sus funciones sin necesidad de obtener ninguna acreditación específica.

Disposición transitoria tercera. *Ingenieros y técnicos de las empresas de seguridad.*

Los ingenieros y técnicos encuadrados, en el momento de entrada en vigor de esta ley, en empresas de seguridad autorizadas para la actividad de instalación y mantenimiento de sistemas de seguridad contemplada en el artículo 5.1.f) podrán continuar desarrollando sus funciones sin necesidad de obtener la acreditación específica a la que se refiere el artículo 19.1.c).

Disposición transitoria cuarta. *Plazos de adecuación.*

1. Las empresas de seguridad privada y sus delegaciones, los despachos de detectives privados y sus sucursales, las medidas de seguridad adoptadas y el material o equipo en uso a la entrada en vigor de esta ley de acuerdo con la normativa anterior, pero que no cumplan, total o parcialmente, los requisitos o exigencias establecidos en esta ley y en sus normas de desarrollo, deberán adaptarse a tales requisitos y exigencias, dentro de los siguientes plazos de adecuación, computados a partir de su entrada en vigor:

a) Dos años respecto a los requisitos nuevos de las empresas de seguridad privada y sus delegaciones y de los despachos de detectives privados y sus sucursales.

b) Diez años para las medidas de seguridad electrónicas de las empresas de seguridad, de los establecimientos obligados y de las instalaciones de los usuarios no obligados.

c) Un año para la obtención de la certificación prevista en el artículo 19.4.

2. Las medidas de seguridad física instaladas con anterioridad a la entrada en vigor de esta ley tendrán una validez indefinida, hasta el final de su vida útil; no obstante, deberán ser

actualizadas en caso de resultar afectadas por reformas estructurales de los sistemas de seguridad de los que formen parte.

3. Los sistemas de seguridad y los elementos de seguridad física, electrónica e informática que se instalen a partir de la entrada en vigor de esta ley deberán cumplir todas las exigencias y requisitos establecidos en la misma y en su normativa de desarrollo.

Disposición transitoria quinta. *Actividad de planificación y asesoramiento.*

1. Las empresas de seguridad autorizadas e inscritas únicamente para la actividad de planificación y asesoramiento contemplada en el artículo 5.1.g) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, dispondrán de un plazo de tres meses, desde la entrada en vigor de esta ley, para solicitar autorización para cualquiera de las actividades enumeradas en el artículo 5.1 de la misma, excepto la contemplada en el párrafo h).

2. Las empresas de seguridad referidas en el apartado anterior que, transcurrido dicho plazo, no hubieran solicitado la mencionada autorización, serán dadas de baja de oficio, cancelándose su inscripción en el Registro Nacional de Seguridad Privada y, en su caso, en el registro autonómico correspondiente.

3. En el caso de las empresas de seguridad que, a la entrada en vigor de esta ley, estuvieran autorizadas e inscritas para la actividad de planificación y asesoramiento y, además, para cualquier otra contemplada en el artículo 5.1, se cancelará de oficio su inscripción y autorización en el Registro Nacional de Seguridad Privada y, en su caso, en el registro autonómico correspondiente únicamente respecto a dicha actividad de planificación y asesoramiento.

4. Las empresas de seguridad referidas en el apartado anterior dispondrán de un plazo de un año, desde la entrada en vigor de esta ley, para adecuar los respectivos importes del seguro de responsabilidad civil u otra garantía financiera, así como del aval o seguro de caución, en función de las actividades para las que continúen autorizadas e inscritas en los registros correspondientes.

5. Los procedimientos administrativos que, a la entrada en vigor de esta ley, se estuvieran tramitando en relación con la solicitud de autorización e inscripción para desarrollar únicamente la referida actividad de planificación y asesoramiento se darán por terminados, procediéndose al archivo de las actuaciones.

6. Los procedimientos administrativos que, a la entrada en vigor de esta ley, se estuvieran tramitando en relación con la solicitud de autorización para desarrollar actividades de seguridad privada entre las que se incluya la referida actividad de planificación y asesoramiento, continuarán su tramitación en relación exclusivamente con el resto de actividades solicitadas.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada la Ley 23/1992, de 30 de julio, de Seguridad Privada, y cuantas normas de igual o inferior rango se opongan a lo dispuesto en esta ley.

2. El Reglamento de Seguridad Privada, aprobado por el Real Decreto 2364/1994, de 9 de diciembre, y el resto de la normativa de desarrollo de la Ley 23/1992, de 30 de julio, y del propio Reglamento mantendrán su vigencia en lo que no contravenga a esta ley.

Disposición final primera. *Título competencial.*

Esta ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública.

Disposición final segunda. *Procedimiento administrativo.*

En todo lo no regulado expresamente en esta ley se aplicará la legislación sobre procedimiento administrativo.

Disposición final tercera. *Desarrollo normativo.*

1. El Gobierno, a propuesta del Ministro del Interior, dictará las disposiciones reglamentarias que sean precisas para el desarrollo y ejecución de lo dispuesto en esta ley, y concretamente para determinar:

a) Los requisitos y características que han de reunir las empresas y entidades objeto de regulación.
b) Las condiciones que deben cumplirse en la realización de actividades de seguridad privada y en la prestación de servicios de esta naturaleza.
c) Las características que han de reunir las medidas de seguridad privada y los medios técnicos y materiales utilizados en las actividades y servicios de seguridad privada.
d) Las funciones, deberes, responsabilidades y cualificación del personal de seguridad privada y del personal acreditado.
e) El régimen de habilitación y acreditación de dicho personal.
f) Los órganos del Ministerio del Interior competentes, en cada caso, para el desempeño de las distintas funciones.

2. Se faculta, asimismo, al Gobierno para actualizar la cuantía de las multas, de acuerdo con las variaciones del indicador público de renta de efectos múltiples.

Disposición final cuarta. *Entrada en vigor.*

Esta ley entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado».

§ 20

Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada

Ministerio de Justicia e Interior
«BOE» núm. 8, de 10 de enero de 1995
Última modificación: 5 de abril de 2014
Referencia: BOE-A-1995-608

A partir del 5 de junio de 2014, esta norma mantiene su vigencia en lo que no contravenga a la Ley 5/2014, de 4 de abril, según establece la disposición derogatoria única de la citada Ley. Ref. BOE-A-2014-3649.
Téngase en cuenta que todas las referencias a la nacionalidad y a la residencia contenidas en este Reglamento se entenderán hechas a la nacionalidad de cualquiera de los Estados miembros de la Unión Europea y a la de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, y a la residencia en el territorio de dichos Estados, conforme establece la disposición adicional tercera del Real Decreto 1123/2001, de 19 de octubre. Ref. BOE-A-2001-21874.

La Ley 23/1992, de 30 de julio, de Seguridad Privada, en su disposición final primera, encomienda al Gobierno dictar las normas reglamentarias que sean precisas para el desarrollo y ejecución de la propia Ley. Por su parte, la disposición final cuarta de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, autoriza igualmente al Gobierno a dictar las normas necesarias para determinar las medidas de seguridad que, de conformidad con lo previsto en el artículo 13 del mismo texto legal, puedan ser impuestas a entidades y establecimientos.

La indudable afinidad de las materias aludidas y la finalidad idéntica de las mismas, constituida por la prevención de los delitos, aconseja desarrollarlas reglamentariamente de forma unitaria, lo que se lleva a cabo mediante el Reglamento de Seguridad Privada, que se aprueba por el presente Real Decreto.

De acuerdo con el mandato conferido por la Ley de Seguridad Privada, se determinan en el Reglamento los requisitos y características de las empresas de seguridad; las condiciones que deben cumplirse en la prestación de sus servicios y en el desarrollo de sus actividades, y las funciones, deberes y responsabilidades del personal de seguridad privada; al tiempo que se determinan los órganos competentes para el desempeño de las distintas funciones administrativas, y se abre el camino para la determinación de las características de los medios técnicos y materiales utilizables.

En relación con la determinación de las facultades que en materia de seguridad privada corresponden a las Comunidades Autónomas competentes para la protección de personas y bienes y para el mantenimiento del orden público, el Reglamento, como no podía ser menos,

se limita a desarrollar lo establecido en la disposición adicional cuarta de la Ley 23/1992, de 30 de julio.

Se continúa así en este ámbito la línea favorable a una interpretación amplia de las atribuciones de las Comunidades Autónomas, en relación con la definición que de la competencia autonómica sobre sus propios servicios policiales y sus funciones ha realizado la jurisprudencia constitucional (más concretamente la Sentencia 104/1989, de 8 de junio).

Desde esta perspectiva, el Reglamento recoge la atribución específica a las Comunidades Autónomas aludidas de funciones ejecutivas de la normativa estatal respecto a la autorización, inspección y sanción de las empresas de seguridad que tengan su domicilio social y su ámbito de actuación en la propia Comunidad Autónoma, respetando así la decisión del legislador, que entiende comprendidas, si quiera sea parcialmente, determinadas competencias sobre seguridad privada en el ámbito de las facultades autonómicas asumidas estatutariamente al amparo del artículo 149.1.29.ª de la Constitución.

En coherencia con lo anterior, la Ley 23/1992 y este Reglamento sientan de forma clara la competencia estatal respecto a aquellas actividades de seguridad privada que, por su ámbito funcional de desarrollo o por estar conectadas con aquélla, no pueden entenderse comprendidas en el ámbito de la competencia autonómica para regular su propia policía destinada al mantenimiento del orden público y a la protección de personas y bienes.

En este sentido la habilitación del personal de seguridad privada, que la Ley 23/1992 no incluyó entre las facultades autonómicas, implica el ejercicio de funciones derivadas de la competencia estatal exclusiva sobre la seguridad pública, sin que aquélla pueda incluirse en la competencia autonómica sobre sus propios servicios policiales, tal y como la define la jurisprudencia constitucional. A mayor abundamiento, se está ante una habilitación para el ejercicio de determinadas funciones en todo el territorio estatal y ante personas que en la mayor parte de los casos pueden desarrollar sus funciones provistas de armas de fuego.

Por lo que respecta a la seguridad en establecimientos e instalaciones, se desarrolla el artículo 13 de la Ley Orgánica sobre Protección de la Seguridad Ciudadana, determinando los servicios y sistemas de seguridad que habrán de adoptar las distintas clases de establecimientos, a cuyo efecto se cuenta con la experiencia acumulada durante los últimos años, adecuándose las medidas de seguridad en entidades y establecimientos públicos y privados al objeto perseguido, teniendo en cuenta las nuevas tecnologías.

Se completa así el ciclo normativo de la seguridad privada, contemplada en su totalidad, poniéndose fin a la dispersión de normas vigentes, dictadas a partir del año 1974, y subsanando las lagunas existentes y los desfases producidos por la propia dinámica de la seguridad privada durante los años transcurridos.

En su virtud, a propuesta del Ministro de Justicia e Interior, con la aprobación del Ministro para las Administraciones Públicas, oído el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 9 de diciembre de 1994,

D I S P O N G O :

Artículo único.

En desarrollo y ejecución de la Ley 23/1992, de 30 de julio, de Seguridad Privada, y del artículo 13 de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, se aprueba el Reglamento de Seguridad Privada, cuyo texto se inserta a continuación.

Disposición adicional primera. *Actividades excluidas.*

Quedan fuera del ámbito de aplicación del Reglamento de Seguridad Privada las actividades siguientes, realizadas por personal distinto del de seguridad privada, no integrado en empresas de seguridad, siempre que la contratación sea realizada por los titulares de los inmuebles y tenga por objeto directo alguna de las siguientes actividades:

a) Las de información en los accesos, custodia y comprobación del estado y funcionamiento de instalaciones, y de gestión auxiliar, realizadas en edificios particulares por porteros, conserjes y personal análogo.

b) En general, la comprobación y control del estado de calderas e instalaciones generales en cualesquiera clase de inmuebles, para garantizar su funcionamiento y seguridad física.

c) El control de tránsito en zonas reservadas o de circulación restringida en el interior de fábricas, plantas de producción de energía, grandes centros de proceso de datos y similares.

d) Las tareas de recepción, comprobación de visitantes y orientación de los mismos, así como las de control de entradas, documentos o carnés privados, en cualquier clase de edificios o inmuebles.

Disposición adicional segunda. *Funcionamiento del Registro General de Empresas de Seguridad.*

El Registro General de Empresas de Seguridad constituido en el Ministerio de Justicia e Interior, al que se refiere el artículo 7 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, funcionará en la unidad orgánica especializada en materia de seguridad privada, dentro de la Comisaría General de Seguridad Ciudadana.

Disposición adicional tercera. *Comisiones de coordinación.*

1. Presididas por el Director general de la Policía y, en su caso, por los Gobernadores Civiles funcionarán comisiones mixtas, central y provinciales, de coordinación de la seguridad privada en el ámbito de competencias de la Administración General del Estado, integradas por representantes de las empresas y entidades obligadas a disponer de medidas de seguridad, y de los trabajadores de los sectores afectados, pudiendo integrarse en ellas asimismo representantes de las Comunidades Autónomas y de las Corporaciones Locales. La organización y funcionamiento de las comisiones serán regulados por Orden del Ministro de Justicia e Interior.

2. En las Comunidades Autónomas con competencias para la protección de las personas y bienes, y para el mantenimiento del orden público con arreglo a los correspondientes Estatutos de Autonomía y a lo previsto en la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, también podrán existir Comisiones Mixtas de coordinación de seguridad privada en el ámbito de dichas competencias, cuya presidencia, composición y funciones sean determinadas por los órganos competentes de las mismas.

3. A las reuniones de dichas comisiones mixtas deberán ser convocados también los representantes o los jefes de seguridad de las empresas de seguridad y los representantes de los trabajadores, cuando vayan a ser tratados temas que afecten a sus servicios o actividades.

4. La convocatoria de las reuniones corresponderá efectuarla a los presidentes de las comisiones, por propia iniciativa o teniendo en cuenta las peticiones de los representantes de las empresas y de los trabajadores.

5. El régimen jurídico de estas comisiones se ajustará a las normas contenidas en el capítulo II del título II, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sin perjuicio de las peculiaridades organizativas que procedan en cada caso.

Disposición adicional cuarta. *Incompatibilidades del personal.*

En aplicación de lo dispuesto en los artículos 1.3 y 11.2 de la Ley 53/1984, de incompatibilidades del personal al servicio de las Administraciones Públicas, el desempeño de puestos de trabajo en dichas Administraciones por el personal incluido en el ámbito de aplicación de dicha Ley será incompatible con el ejercicio de las siguientes actividades:

a) El desarrollo de funciones propias del personal de seguridad privada.

b) La pertenencia a Consejos de Administración u órganos rectores de empresas de seguridad.

c) El desempeño de puestos de cualquier clase en empresas de seguridad.

Disposición adicional quinta. *Exclusión de las empresas relacionadas con equipos técnicos de seguridad.*

1. De conformidad con lo dispuesto en la disposición adicional sexta de la Ley 23/1992, de 30 de julio, de Seguridad Privada, introducida por la Ley 25/2009, de 22 de diciembre, los prestadores de servicios o las filiales de las empresas de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarmas, quedan excluidos de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5 de la Ley 23/1992, de 30 de julio, y sin perjuicio de otras legislaciones específicas que pudieran resultar de aplicación.

2. Las empresas de seguridad privada que, además de dedicarse a una o a varias de las actividades contempladas en el artículo 5 de la Ley 23/1992, de 30 de julio, se dediquen a la instalación de aparatos, dispositivos y sistemas de seguridad que no incluyan la conexión a centrales de alarma, sólo estarán sometidas a la legislación de seguridad privada en lo que se refiere a la prestación de las actividades y servicios regulados en el citado artículo, quedando la actividad de instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad no conectados a centrales de alarma sometida a las reglamentaciones técnicas que le sean de aplicación, y en particular a la normativa aplicable en materia de homologación de productos.

Disposición transitoria primera. *Plazo de adaptación a la Ley.*

El plazo de un año concedido por la disposición transitoria primera de la Ley 23/1992, de 30 de julio, para la adaptación a los requisitos o exigencias establecidos en la propia Ley y en sus normas de desarrollo, se contará:

a) Con carácter general, respecto a los requisitos nuevos de las empresas necesitados de concreción reglamentaria, y a las medidas de seguridad adoptadas con anterioridad, a partir de la fecha de promulgación del Reglamento de Seguridad Privada.

b) Respecto al material o equipo y a aquellas materias que, con arreglo a lo dispuesto en el mencionado Reglamento, requieran concreciones, determinaciones o aprobaciones complementarias por parte del Ministerio de Justicia e Interior, desde la fecha en que entren en vigor las correspondientes Ordenes de regulación o Resoluciones de homologación ministeriales.

c) Respecto a las materias no comprendidas en los párrafos anteriores, desde la fecha de promulgación de la Ley.

Disposición transitoria segunda. *Efectos de la adaptación y de la no adaptación.*

1. Las empresas de seguridad inscritas en el Registro, que se adapten a lo previsto en la Ley y en el Reglamento de Seguridad Privada, podrán conservar el mismo número de inscripción que tuvieren anteriormente.

2. Transcurrido el plazo de un año desde la promulgación del Reglamento de Seguridad Privada, otorgado a las empresas a efectos de adecuación a los requisitos establecidos para su inscripción en el Registro de empresas, a las que no lo hubieren hecho dentro del indicado plazo se las considerará dadas de baja en dicho Registro, estimándose cancelada su inscripción, lo que se notificará formalmente a las empresas interesadas.

Disposición transitoria tercera. *Adaptación de empresas de seguridad no inscritas anteriormente.*

1. También dispondrán del plazo de un año, contado en la forma prevista en los apartados a) y b) de la disposición transitoria primera, para adaptarse a los requisitos o exigencias propios de las empresas de seguridad establecidos en la Ley de Seguridad Privada, en el Reglamento de dicha Ley y en sus normas de desarrollo, todas aquellas empresas no inscritas en el Registro de Empresas de Seguridad, dedicadas al transporte y distribución de explosivos o a otras ramas de actividad económica y que, con anterioridad a la entrada en vigor de la Ley y con arreglo a las normas entonces vigentes, hubieran venido

prestando a terceros los servicios atribuidos por la Ley de Seguridad Privada, con carácter exclusivo, a las empresas de seguridad.

2. Mientras estuvieran realizando los trámites de adaptación durante el plazo indicado, las referidas empresas tendrán la consideración de empresas de seguridad, a efectos de lo dispuesto en el artículo 12.1 de la Ley de Seguridad Privada, en relación con los vigilantes jurados de seguridad, los guardas jurados de explosivos y demás personal de seguridad privada que se encuentren prestando servicio en las mismas y lo hubieran estado prestando en la fecha de entrada en vigor de la Ley.

Disposición transitoria cuarta. *Cómputo de capital y reservas.*

A efectos de integrar los distintos niveles de recursos propios exigidos por el Reglamento de Seguridad Privada, las empresas de seguridad constituidas con anterioridad a la promulgación de la Ley 23/1992 podrán computar, además de su capital social, las reservas efectivas y expresas que consten en el balance cerrado el 31 de diciembre de 1992 y debidamente aprobado por el órgano social competente.

Disposición transitoria quinta. *Plazos de adecuación de medidas de seguridad.*

1. Sin perjuicio de lo dispuesto con carácter general en la disposición transitoria primera de la Ley 23/1992, de 30 de julio, las medidas y sistemas de seguridad instalados antes de la fecha de entrada en vigor del Reglamento de dicha Ley o de las normas que lo desarrollen, se adecuarán a los requisitos que establezcan, una vez transcurridos los siguientes plazos, a partir de aquella fecha:

A. Medidas de seguridad físicas.

a) Empresas de seguridad:

1.º Un año para instalar, en la sede social y en las delegaciones de las empresas que se dediquen a la instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, la zona de seguridad destinada a garantizar la custodia de la información que manejaren.

2.º Un año para que las empresas de centrales de alarmas adecuen el acristalamiento de sus centros de control a los niveles de seguridad que se determinen por el Ministerio de Justicia e Interior.

b) Empresas, entidades y establecimientos obligados a la adopción de medidas de seguridad:

1.º Cinco años para instalar la puerta blindada a que se refiere el artículo 127.1.d) del Reglamento de Seguridad Privada.

2.º Cinco años para las medidas correspondientes a cámaras acorazadas y cámaras de cajas de alquiler.

No será necesaria la adecuación exigida en esta disposición transitoria a los requisitos establecidos por las normas de desarrollo del Reglamento de Seguridad Privada, de las cámaras acorazadas de efectivo que tengan por finalidad exclusiva la de proteger el encaje diario necesario para el funcionamiento de la oficina correspondiente. También será necesaria la adecuación de los compartimentos de alquiler de las cámaras, ni la de las cajas fuertes o armarios blindados en que se ubiquen compartimentos de alquiler.

Las cámaras acorazadas de efectivo, con excepción de las incluidas en el párrafo anterior, y las cámaras de cajas de alquiler instaladas con anterioridad a la fecha de entrada en vigor de las normas de desarrollo del Reglamento de Seguridad Privada, quedarán eximidas del cumplimiento del deber de adaptación a las medidas de seguridad establecidas, cuando los servicios policiales competentes verifiquen la imposibilidad física de llevar a cabo tal adaptación, y siempre que las citadas cámaras se doten de las medidas complementarias de carácter electrónico que se determinen."

Las medidas correspondientes a cámaras acorazadas de efectivo y cámaras de cajas de alquiler reguladas en el Reglamento de Seguridad Privada y normas que lo desarrollen, serán exigibles a aquéllas que se instalen por primera vez a partir de la fecha de entrada en vigor de las citadas normas de desarrollo.

3.º Cinco años para que las oficinas de farmacia instalen el dispositivo a que se refiere el artículo 131.1 de dicho Reglamento.

4.º Cinco años para que las Administraciones de Lotería, Despachos de Apuestas Mutuas y locales de juegos de azar se adapten a lo dispuesto en el artículo 132.1 y 2 y en el artículo 133 del Reglamento, respectivamente.

B) Sistemas de seguridad electrónicos:

1.º Un año para los instalados en empresas de seguridad.

2.º Dos años para los correspondientes a cámaras acorazadas o cámaras de cajas de alquiler.

3.º Un año para que, respecto a los instalados por empresas no homologadas y conectados con centrales de alarmas, se acredite ante éstas, mediante certificado de empresa habilitada en el Registro para este tipo de actividades, que la instalación se ajusta a lo dispuesto en los artículos 40, 42 y 43 del Reglamento. Transcurrido el plazo de un año sin que se haya presentado el certificado, la empresa de central de alarmas procederá a la desconexión del sistema.

4.º Cinco años para el resto de sistemas de seguridad electrónicos.

2. Los sistemas de seguridad físicos de los cajeros automáticos y cajas fuertes, regulados en el Reglamento de Seguridad Privada y normas que lo desarrollen, serán exigibles a aquellos que se instalen a partir del año siguiente a la fecha de su entrada en vigor.

Disposición transitoria sexta. *Plazo de incorporación de armeros.*

1. Transcurrido un plazo de un año, contado desde la fecha de entrada en vigor del Reglamento de Seguridad Privada, los lugares en los que se presten servicios de vigilantes de seguridad con armas deberán disponer de los armeros a que se refiere su artículo 25.

2. Durante dicho plazo, respecto a los lugares que no dispongan de armero, será de aplicación lo dispuesto en el artículo 82, apartado 2.

Disposición transitoria séptima. *Plazo de utilización de vehículos blindados.*

Los vehículos blindados utilizados por las empresas de transporte y distribución, cuyas características no se correspondan con las que determine el Ministerio de Justicia e Interior, podrán ser utilizados durante un plazo de un año, contado a partir de la entrada en vigor de las normas que al efecto se dicten. Transcurrido dicho plazo, todos los vehículos que se utilicen para esta actividad habrán de ajustarse a lo dispuesto en las citadas normas.

Disposición transitoria octava. *Disposiciones relativas a la habilitación del personal.*

A los efectos de cómputo de los plazos establecidos en las disposiciones transitorias tercera y cuarta de la Ley 23/1992, de 30 de julio, se considerarán disposiciones de desarrollo reglamentario relativas a la habilitación para el ejercicio de funciones de seguridad privada, además de las contenidas al respecto en el Reglamento de Seguridad Privada:

a) Las de concreción, determinación o aprobación de distintos aspectos, encomendadas expresamente en distintos preceptos al Ministerio de Justicia e Interior.

b) Las de regulación de la apertura y funcionamiento de los centros de formación y perfeccionamiento de personal de seguridad privada.

c) Las de regulación de las pruebas necesarias para la obtención de la tarjeta de identidad profesional del personal de seguridad privada.

Disposición transitoria novena. *Personal ya habilitado.*

1. Los vigilantes jurados de seguridad, guardas jurados de explosivos, guardas particulares jurados del campo, guardas de caza y guardapescas jurados marítimos que en la fecha de entrada en vigor de la Ley 23/1992 reunieran las condiciones exigibles para la prestación de los correspondientes servicios con arreglo a la regulación anterior a aquélla podrán seguir desempeñando las funciones para las que estuviesen documentados, sin necesidad de obtener la habilitación a que se refiere el artículo 10 de la citada Ley. Lo

dispuesto en este apartado será en general aplicable a cualquier clase de personal que, independientemente de su denominación, viniera realizando funciones propias de personal de seguridad privada.

2. Los detectives privados que se encontrasen acreditados como tales en la fecha de promulgación de la indicada Ley podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado.

Disposición transitoria décima. *Canje de acreditaciones de personal.*

1. El personal a que se refiere la disposición transitoria anterior, que en la fecha de entrada en vigor de la Orden de aprobación de los modelos de tarjetas de identidad profesional continúe reuniendo las condiciones exigibles para la prestación de los correspondientes servicios, deberá canjear a partir de dicha fecha sus títulos-nombramientos, licencias, tarjetas de identidad o acreditaciones, por las indicadas tarjetas de identidad profesional, en los siguientes plazos:

a) Dos años, el personal mencionado en el apartado 1 de la disposición transitoria anterior.

b) Un año, los detectives privados.

2. Los jefes de seguridad que en la fecha citada en el apartado anterior se hallasen desempeñando sus funciones, con la conformidad de la Dirección de la Seguridad del Estado o del órgano competente del Ministerio de Justicia e Interior, deberán canjear su acreditación en el plazo de dos años, contado a partir de la indicada fecha.

3. Las nuevas acreditaciones se expedirán al personal mencionado, con carácter gratuito.

Disposición transitoria undécima. *Auxiliares de detectives acreditados.*

1. Los auxiliares de detective que se encontrasen acreditados como tales en la fecha de promulgación de la Ley 23/1992 podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado, durante cuyo plazo habrán de figurar en el Registro especial regulado en el artículo 104 del Reglamento de dicha Ley.

2. Para poder ejercer las actividades previstas en el artículo 19.1 de la citada Ley, habrán de superar durante el expresado plazo las pruebas de aptitud técnico-profesional que establezca el Ministerio de Justicia e Interior y que estarán a un nivel concordante con la titulación académica exigida para el ejercicio de las indicadas actividades, lo que les habilitará para poder obtener la tarjeta de identidad profesional de detective privado.

Disposición transitoria duodécima. *Investigadores o informadores en ejercicio.*

1. Los investigadores o informadores que acrediten oficialmente el ejercicio profesional durante dos años con anterioridad a la fecha de promulgación de la Ley 23/1992, podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado.

2. Para poder ejercer las actividades previstas en el artículo 19.1 de la citada Ley, habrán de superar, durante el expresado plazo, las pruebas de aptitud técnico-profesional que establezca el Ministerio de Justicia e Interior, teniendo en cuenta la experiencia obtenida en el desarrollo anterior de sus funciones, lo que les habilitará para poder obtener la tarjeta de identidad profesional de detective privado.

Disposición transitoria decimotercera. *Uniformidad del personal.*

Los vigilantes de seguridad y los guardas particulares del campo, en sus distintas modalidades, podrán seguir utilizando la uniformidad que tuvieran autorizada con anterioridad, hasta que transcurra el plazo de dos años siguiente a la fecha de entrada en

vigor de las normas que dicte el Ministerio de Justicia e interior al respecto, debiendo regirse por ellas finalizado dicho plazo.

Disposición transitoria decimocuarta. *Libros-Registros abiertos.*

Las empresas de seguridad y los detectives privados podrán seguir utilizando los Libros-Registros que tuvieren abiertos, hasta que transcurra el plazo de un año, a partir de la publicación de los nuevos modelos que se aprueben con arreglo a lo dispuesto en el Reglamento de Seguridad Privada. Finalizado dicho plazo, los Libros-Registros deberán ser sustituidos por los previstos en el Reglamento.

Disposición derogatoria única. *Alcance de la derogación normativa.*

1. Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en el presente Real Decreto así como en el Reglamento que por el mismo se aprueba y especialmente:

a) El Real Decreto 880/1981, de 8 de mayo, sobre prestación privada de servicios de seguridad.
b) El Real Decreto 629/1978, de 10 de marzo, por el que se regula la función de los vigilantes jurados de seguridad, modificado por Real Decreto 738/1983, de 23 de febrero.
c) El Real Decreto 760/1983, de 30 de marzo, por el que se regula el nombramiento y ejercicio de las funciones de los guardas jurados de explosivos.
d) El Real Decreto de 8 de noviembre de 1849, por el que se reglamentan, entre otros, los nombramientos y funciones de los guardas particulares del campo.
e) Los apartados 2, 3 y 4 del artículo 44 del Reglamento de ejecución de la Ley de Caza, aprobado por Decreto 506/1971, de 25 de marzo.
f) El Decreto 1583/1974, de 25 de abril, por el que se aprueba el Reglamento de guardapescas jurados marítimos de establecimientos de acuicultura.
g) El Real Decreto 1338/1984, de 4 de julio, sobre Medidas de Seguridad en entidades y establecimientos públicos y privados.
h) La Orden del Ministerio del Interior, de 20 de enero de 1981, por la que se regula la profesión de detective privado.

2. No obstante lo dispuesto en el apartado anterior, permanecerán en vigor las normas sobre habilitación o nombramiento del personal de seguridad privada, hasta el momento que se determine por las normas y actos de ejecución y desarrollo del Reglamento de Seguridad Privada en el que pueda tener efectividad el sistema de formación y habilitación de dicho personal, regulado en dicho Reglamento y en los aludidos normas y actos.
3. Asimismo, seguirán exigiéndose las especificaciones o requisitos de carácter técnico, previstos en la legislación vigente, hasta que entren en vigor las correspondientes normas de desarrollo del Reglamento de Seguridad Privada.

Disposición final primera. *Disposiciones de ejecución.*

Se autoriza al Ministro de Justicia e Interior y al Ministro de Industria y Energía, previo informe, en su caso, del Ministro de Agricultura, Pesca y Alimentación y de las Comunidades Autónomas con competencias en materia de seguridad privada, para dictar, en la esfera de sus respectivas competencias, las disposiciones que sean necesarias para la ejecución y aplicación de lo dispuesto en el presente Real Decreto y en el Reglamento de Seguridad Privada.

Disposición final segunda. *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE SEGURIDAD PRIVADA

TITULO I

Empresas de Seguridad

CAPITULO I

Inscripción y autorización

Artículo 1. *Servicios y actividades de seguridad privada.*

1. Las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades:

a) Vigilancia y protección de bienes, establecimientos, espectáculos, certámenes o convenciones.

b) Protección de personas determinadas, previa la autorización correspondiente.

c) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen o por su peligrosidad, puedan requerir protección especial, sin perjuicio de las actividades propias de las entidades financieras.

d) Transporte y distribución de los objetos a que se refiere el apartado anterior, a través de los distintos medios, realizándolos, en su caso, mediante vehículos cuyas características serán determinadas por el Ministerio de Justicia e Interior, de forma que no puedan confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad.

e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad conectados a centrales de alarma.

f) Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos.

g) Planificación y asesoramiento de las actividades de seguridad (artículo 5.1 de la Ley de Seguridad Privada).

2. Dentro de lo dispuesto en los párrafos c) y d) del apartado anterior, se comprenden la custodia, los transportes y la distribución de explosivos, sin perjuicio de las actividades propias de las empresas fabricantes, comercializadoras y consumidoras de dichos productos.

3. Las empresas de seguridad no podrán dedicarse a la fabricación de material de seguridad, salvo para su propia utilización, explotación y consumo, ni a la comercialización de dicho material. Y las empresas dedicadas a estas actividades no podrán usar, como denominación o calificativo de su naturaleza, la expresión «Empresa de Seguridad».

4. Son de carácter privado las empresas, el personal y los servicios de seguridad objeto del presente Reglamento, cuyas actividades tienen la consideración legal de actividades complementarias y subordinadas respecto a las de seguridad pública.

Artículo 2. *Obligatoriedad de la inscripción y de la autorización o reconocimiento.*

1. Para la prestación de los servicios y el ejercicio de las actividades enumerados en el artículo anterior, las empresas deberán reunir los requisitos determinados en el artículo 7 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, ser autorizadas siguiendo el procedimiento regulado en los artículos 4 y siguientes de este reglamento y hallarse inscritas en el Registro de Empresas de Seguridad existente en el Ministerio del Interior.

2. Las empresas de seguridad autorizadas para la prestación de servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión

Europea o de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, serán reconocidas e inscritas en el citado Registro una vez que acrediten su condición de empresa de seguridad y el cumplimiento de los requisitos establecidos en los artículos 5, 6 y 7 de este reglamento. A tal efecto, se tendrán en cuenta los requisitos ya acreditados en cualquiera de dichos Estados y, en consecuencia, no será necesaria nueva cumplimentación de los mismos.

3. En el Registro, con el número de orden de inscripción y autorización de la empresa, figurará su denominación, número de identificación fiscal, fecha de autorización, domicilio, clase de sociedad o forma jurídica, actividades para las que ha sido autorizada, ámbito territorial de actuación y representante legal, así como las modificaciones o actualizaciones de los datos enumerados.

Artículo 3. *Ambito territorial de actuación.*

Las empresas de seguridad limitarán su actuación al ámbito geográfico, estatal o autonómico, para el que se inscriban en el Registro.

Artículo 4. *Procedimiento de autorización.*

1. El procedimiento de autorización constará de tres fases, que requerirán documentaciones específicas y serán objeto de actuaciones y resoluciones sucesivas, considerándose únicamente habilitadas de forma definitiva las empresas de seguridad cuando obtengan la autorización de entrada en funcionamiento.

2. No obstante lo dispuesto en el apartado anterior, a petición de la empresa interesada podrán desarrollarse de forma conjunta, sin solución de continuidad, la primera y la segunda de las fases indicadas, e incluso la totalidad del procedimiento de autorización.

En este caso, junto a la solicitud deberá acompañarse la documentación correspondiente a las diferentes fases parar las que se solicite la tramitación conjunta.

Artículo 5. *Documentación.*

1. El procedimiento de autorización se iniciará a solicitud de la sociedad o persona interesada, que deberá acompañar los siguientes documentos:

a) Fase inicial, de presentación:

1.º Si se trata de sociedades, copia auténtica de la escritura pública de constitución, en la que deberá constar que la sede social o establecimiento se encuentra en un Estado miembro de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo, su objeto social, que habrá de ser exclusivo y coincidente con uno o más de los servicios o actividades a que se refiere el artículo 1 de este reglamento, titularidad del capital social, y certificado de la inscripción o nota de inscripción reglamentaria de la sociedad en el Registro Mercantil o, en su caso, en el Registro de Cooperativas que corresponda, o documento equivalente en el caso de sociedades constituidas en cualquiera de dichos Estados.

2.º Declaración de la clase de actividades que pretende desarrollar y ámbito territorial de actuación.

No podrá inscribirse en el Registro ninguna empresa cuya denominación induzca a error con la de otra ya inscrita o con la de órganos o dependencias de las Administraciones Públicas, pudiendo formularse consultas previas al Registro, para evitar tal error.

b) Segunda fase, de documentación de requisitos previos:

1.º Inventario de los medios materiales de que disponga para el ejercicio de sus actividades.

2.º Documento acreditativo del título en virtud del cual dispone de los inmuebles en que se encuentre el domicilio social y demás locales de la empresa, cuando aquéllos estén ubicados en España.

3.º Si se trata de sociedades, composición personal de los órganos de administración y dirección.

c) Tercera fase, de documentación complementaria y resolución:

1.º En su caso, certificado de inscripción de la escritura pública de constitución de la sociedad en el Registro Mercantil, o en el Registro de Cooperativas correspondiente o documento equivalente, si no se hubiera presentado con anterioridad.

2.º Certificado acreditativo de la instalación de un sistema de seguridad, de las características que determine el Ministerio del Interior.

3.º Documento acreditativo del alta en el Impuesto de Actividades Económicas.

4.º Memoria explicativa de los planes de operaciones a que hayan de ajustarse las diversas actividades que pretenden realizar.

5.º Relación del personal, con expresión de su categoría y del número del documento nacional de identidad, o, en el caso de nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, del número de identidad de extranjero. Cuando no haya obligación de obtener este último, se expresará el número del documento de identidad equivalente.

6.º Documentación acreditativa de las suscripción de un contrato de seguro de responsabilidad civil, aval u otra garantía financiera contratada con entidad debidamente autorizada de cualquiera de los Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, con el objeto de cubrir, hasta la cuantía de los límites establecidos en el anexo del presente reglamento, la responsabilidad civil que por los daños en las personas o los bienes pudieran derivarse de la explotación de la actividad o actividades para las que la empresa esté autorizada.

A las empresas legalmente autorizadas en otro Estado miembro de la Unión Europea o en un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para ejercer actividades o prestar servicios de seguridad privada en dicho Estado y que pretendan ejercer tales actividades o servicios en España, se les tendrá en cuenta el contrato de seguro de responsabilidad civil, aval u otra garantía financiera, que hubieran suscrito a los mismos efectos en cualquiera de dichos Estados, siempre que el mismo cumpla los requisitos establecidos en este apartado.

Si el seguro de responsabilidad civil, aval u otra garantía financiera suscrito en cualquiera de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo lo fuese por cuantía inferior a la exigida a las empresas españolas por la vigente normativa de seguridad privada, la empresa obligada a su prestación deberá constituir nuevo seguro, aval o garantía complementarios o ampliar el ya suscrito hasta alcanzar dicha cuantía.

7.º Documentación acreditativa de haber constituido garantía, en la forma y condiciones prevenidas en el artículo 7 de este reglamento.

2. Los documentos prevenidos en los apartados anteriores se presentarán adaptados para acreditar el cumplimiento de los requisitos específicos que para cada tipo de actividad se exigen a las empresas de seguridad, con arreglo a lo dispuesto en el anexo de este reglamento.

3. Sin perjuicio de las funciones de inspección y control que corresponden a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía) en materia de seguridad privada, el preceptivo informe del Cuerpo de la Guardia Civil sobre idoneidad de instalación de los armeros que, en su caso, hayan de tener las empresas de seguridad, deberá ser emitido a instancia del Cuerpo Nacional de Policía e incorporado oportunamente al expediente de inscripción.

Artículo 6. *Habilitación múltiple.*

Las empresas que pretendan dedicarse a más de una de las actividades o servicios enumerados en el artículo 1 de este reglamento, habrán de acreditar los requisitos generales, así como los específicos que pudieran afectarles, con las siguientes peculiaridades:

a) El que se refiere a Jefe de Seguridad, que podrá ser único para las distintas actividades.

b) Los relativos a póliza de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada, y a la garantía a la que se refiere el artículo 7 de este reglamento: Si van a realizar dos actividades o servicios, justificarán la mayor de las

cantidades exigidas por cada uno de los dos conceptos. Si pretenden realizar más de dos actividades, la correspondiente póliza de responsabilidad civil, aval u otra garantía financiera, y la garantía regulada en el artículo 7, se incrementarán en una cantidad igual al 25 por ciento de las exigidas para cada una de las restantes clases de servicios o actividades.

Artículo 7. *Constitución de garantía.*

1. Las empresas de seguridad habrán de constituir una garantía en la Caja General de Depósitos o en organismo de naturaleza similar de cualquier Estado miembro de la Unión Europea o Estado parte en el Acuerdo sobre el Espacio Económico Europeo, a disposición de las autoridades con competencias sancionadoras en la materia, con el fin de atender a las responsabilidades que deriven del funcionamiento de la empresas por infracciones a la normativa de seguridad privada.

2. En el caso de que la garantía se constituya en la Caja General de Depósitos, se hará en alguna de las modalidades previstas en la normativa reguladora de dicho organismo, con los requisitos establecidos en la misma.

3. La garantía deberá mantenerse por la cuantía máxima de su importe durante todo el período de vigencia de la autorización, con cuya finalidad las cantidades que, en su caso, se hubieren detraído a los efectos previstos en el apartado 1 de este artículo habrán de reponerse en el plazo de un mes a contar desde la fecha en que hubieren ejecutado los correspondientes actos de disposición.

4. Las empresas legalmente autorizadas en otro Estado miembro de la Unión Europea o en un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para ejercer actividades o prestar servicios de seguridad privada en dicho Estado y que pretendan ejercer tales actividades o servicios en España, podrán constituir la garantía a que se refieren los apartados anteriores en los organismos o entidades autorizados para ello de cualquiera de dichos Estados, siempre que la misma se encuentre a disposición de las autoridades españolas para atender a las responsabilidades que deriven del funcionamiento de la empresa por infracciones a la normativa de seguridad privada.

A las empresas a las que se refiere el párrafo anterior, se les tendrá en cuenta la garantía que, en su caso, hubieran suscrito a los mismos efectos en cualquier Estado miembro de la Unión Europea o parte en el Acuerdo sobre el Espacio Económico Europeo, siempre que cumpla los requisitos mencionados en los apartados anteriores y su cuantía sea equivalente a la exigida a las empresas españolas en virtud de lo dispuesto en el anexo de este reglamento.

Si la garantía depositada en cualquiera de dichos Estados fuese de cuantía inferior a la exigida a las empresas españolas por la vigente normativa de seguridad privada, la empresa depositante deberá constituir nueva garantía complementaria o ampliar la ya suscrita hasta alcanzar dicha cuantía.

Artículo 8. *Subsanación de defectos.*

Si la solicitud inicial, o las que inicien las fases sucesivas cuando el procedimiento conste de dos o tres fases, fueran defectuosas o incompletas, se requerirá al solicitante para que subsane la falta o acompañe los documentos preceptivos, con apercibimiento de que, en caso contrario y una vez transcurridos diez días sin cumplimentar el requerimiento, se le tendrá por desistido y se archivará el expediente.

Artículo 9. *Resoluciones y recursos.*

1. La Administración actuante resolverá motivadamente las distintas fases del procedimiento dentro del plazo de dos meses a partir de la fecha de entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, notificándose a la persona o entidad interesada, con especificación, respecto a la inscripción y autorización, de la actividad o actividades que pueden desarrollar, ámbito territorial de actuación y número de inscripción y autorización asignado.

2. Cuando, dentro del mismo plazo de dos meses determinado en el apartado anterior, se entendiese en cualquiera de las fases del procedimiento que la empresa no reúne los

requisitos necesarios, se resolverá denegando la solicitud, con indicación de los recursos que pueden utilizarse contra la denegación.

3. No obstante lo dispuesto en el apartado anterior, si venciese el plazo de resolución y el órgano competente no la hubiese dictado expresamente, podrá entenderse desestimada la solicitud, pudiendo el interesado interponer contra dicha desestimación presunta los recursos procedentes.

Artículo 10. *Coordinación registral.*

1. El Registro establecido en el Ministerio de Justicia e Interior constituirá el Registro General de Empresas de Seguridad, al cual, aparte de la información correspondiente a las empresas que en el mismo se inscriban, se incorporará la relativa a las empresas inscritas en los registros de las Comunidades Autónomas con competencia en la materia.

2. A efectos de lo dispuesto en el apartado anterior, los órganos competentes de las mencionadas Comunidades Autónomas deberán remitir oportunamente al Registro General de empresas de seguridad copia de las inscripciones y anotaciones que efectúen sobre las empresas de seguridad que inscriban y autoricen, así como de sus modificaciones y cancelación.

3. Toda la información y documentación incorporadas al Registro General de Empresas de Seguridad estará a disposición de los órganos competentes de las Comunidades Autónomas para el ejercicio de sus funciones en materia de seguridad privada.

4. Los sistemas de numeración de los Registros, General y Autonómicos, de empresas de seguridad se determinarán coordinadamente, de forma que el número de inscripción de una empresa de seguridad no pueda coincidir con el de ninguna otra.

CAPITULO II

Modificaciones de inscripción y cancelación

Sección 1.ª Modificaciones de inscripción

Artículo 11. *Supuestos de modificación.*

1. Cualquier variación de los datos incorporados al Registro de empresas de seguridad, enumerados en el artículo 2.3 de este Reglamento, deberá ser objeto del correspondiente expediente de modificación.

2. Las empresas de seguridad podrán solicitar las modificaciones de su inscripción referidas a dichos datos, y en especial a la ampliación o reducción de actividades o de ámbito territorial de actuación.

3. En cualquiera de los supuestos de modificación, los requisitos necesarios, la documentación a aportar y la tramitación del procedimiento deberán atenerse a lo dispuesto en el capítulo anterior y en el anexo de este Reglamento.

4. Si en el momento de la solicitud o durante la tramitación de la misma, a la empresa se le siguiera expediente administrativo por pérdida de los requisitos, recursos humanos o medios materiales o técnicos que permitieron la inscripción o autorización, los dos procedimientos serán objeto de acumulación y de resolución conjunta.

Sección 2.ª Cancelación

Artículo 12. *Causas de cancelación.*

1. Los requisitos, recursos humanos y medios materiales y técnicos exigidos para la inscripción y autorización de las empresas de seguridad deberán mantenerse durante todo el tiempo de vigencia de la autorización.

2. La inscripción de empresas de seguridad para el ejercicio de las actividades o la prestación de servicios a que se refiere el artículo 1 de este Reglamento se cancelará, por el Ministro de Justicia e Interior, por las siguientes causas:

a) Petición propia.

b) Pérdida de alguno de los requisitos, recursos humanos y medios materiales o técnicos exigidos en el capítulo anterior y en el anexo del presente Reglamento.

c) Cumplimiento de la sanción de cancelación.

d) Inactividad de la empresa de seguridad durante el plazo de un año.

Artículo 13. *Efectos de la cancelación.*

1. La cancelación de la inscripción de empresas de seguridad determinará la liberación de la garantía regulada en el artículo 7 de este reglamento, una vez atendidas las responsabilidades a que se refiere el apartado 1 de dicho artículo.

2. No se podrá efectuar la liberación de la garantía cuando la empresa tenga obligaciones económicas pendientes con la Administración derivadas del funcionamiento de la empresa por infracciones a la normativa de seguridad privada, o cuando se le instruya expediente sancionador, hasta su resolución y, en su caso, hasta el cumplimiento de la sanción.

3. No obstante, podrá reducirse la garantía, teniendo en cuenta el alcance previsible de las obligaciones y responsabilidades pendientes.

4. En el supuesto de cancelación por inactividad, la reanudación de la actividad requerirá la instrucción y resolución de un nuevo procedimiento de autorización.

CAPITULO III

Funcionamiento

Sección 1.ª Disposiciones comunes

Artículo 14. *Obligaciones generales.*

1. En el desarrollo de sus actividades, las empresas de seguridad vienen obligadas al especial auxilio y colaboración con las Fuerzas y Cuerpos de Seguridad. A estos efectos deberán comunicar a dichas Fuerzas y Cuerpos cualesquiera circunstancias e informaciones relevantes para la prevención, el mantenimiento o el restablecimiento de la seguridad ciudadana, así como los hechos delictivos de que tuvieren conocimiento en el desarrollo de dichas actividades.

Las empresas de seguridad deberán comunicar las altas y bajas del personal de seguridad privada de que dispongan a las dependencias correspondientes de las Fuerzas y Cuerpos de Seguridad, dentro del plazo de cinco días siguientes a la fecha en que se produzcan.

2. Deberá realizarse siempre con las debidas garantías de seguridad y reserva la prestación de los servicios de protección de personas, depósito, custodia y tratamiento de objetos valiosos, y especialmente los relativos a transporte y distribución de objetos valiosos y de explosivos u otros objetos peligrosos, en lo que respecta a su programación así como a su itinerario.

3. Los servicios y actividades de seguridad deberán ser realizados directamente por el personal de la empresa contratada para su prestación, no pudiendo ésta subcontratarlos con terceros, salvo que lo haga con empresas inscritas en los correspondientes Registros y autorizadas para la prestación de los servicios o actividades objeto de subcontratación, y se cumplan los mismos requisitos y procedimientos prevenidos en este Reglamento para la contratación. La subcontratación no producirá exoneración de responsabilidad de la empresa contratante.

4. No será exigible el requisito de identidad de dedicación, en el supuesto de subcontratación con empresas de vigilancia y protección de bienes, previsto en el artículo 49.4.

Artículo 15. *Comienzo de actividades.*

Una vez inscritas y autorizadas, y antes de entrar en funcionamiento las empresas de seguridad habrán de comunicar la fecha de comienzo de sus actividades a la Dirección General de la Policía, que informará a los Gobiernos Civiles y a las dependencias periféricas

de la misma o a las de la Dirección General de la Guardia Civil del lugar en que radiquen. Las empresas que se dediquen a la explotación de centrales de alarmas, deberán dar cuenta, además, de las fechas de efectividad de las distintas conexiones a las dependencias policiales a las que corresponda dar respuesta a las alarmas.

Artículo 16. *Publicidad de las empresas.*

1. El número de orden de inscripción en el Registro que le corresponda a cada empresa deberá figurar en los documentos que utilice y en la publicidad que desarrolle.

2. Ninguna empresa podrá realizar publicidad relativa a cualquiera de las actividades y servicios a que

hace referencia el artículo 1 de este Reglamento, sin hallarse previamente inscrita en el Registro y autorizada para entrar en funcionamiento.

Artículo 17. *Apertura de sucursales.*

1. Las empresas de seguridad que pretendan abrir delegaciones o sucursales lo solicitarán a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), acompañando los siguientes documentos:

a) Inventario de los bienes materiales que se destinan al ejercicio de las actividades en la delegación o sucursal.

b) Documento acreditativo del título en virtud del cual se dispone del inmueble o inmuebles destinados a la delegación o sucursal.

c) Relación del personal de la delegación o sucursal, con expresión de su cargo, categoría y del número del documento nacional de identidad o, en el caso de nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, del número de identidad de extranjero. Cuando no haya obligación de obtener este último, se expresará el número del documento de identidad equivalente.

2. Las empresas de seguridad deberán abrir delegaciones o sucursales, dando conocimiento a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), con aportación de los documentos reseñados en el apartado anterior, en las Ciudades de Ceuta y Melilla o en las provincias en que no radique su sede principal, cuando realicen en dichas ciudades o provincias alguna de las siguientes actividades:

a) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, así como custodia de objetos valiosos, explosivos u objetos peligrosos. Estas delegaciones deberán contar con los requisitos de dotación de vigilantes de seguridad, armero o caja fuerte, y cámara acorazada y locales anejos, a que se refieren los apartados 3.1.B) y 3.1.C), c) y d) del anexo para objetos valiosos y peligrosos, y con los de dotación de vigilantes de seguridad y armero o caja fuerte, a que se refieren los apartados 3.2.B) y 3.2.C), c) del anexo, respecto a explosivos.

No obstante, cuando la cantidad a custodiar por dichas delegaciones o sucursales no supere los 601.012 euros, siempre que al menos el cincuenta por ciento sea en moneda fraccionaria, la cámara acorazada podrá ser sustituida por una caja fuerte con las características determinadas por el Ministerio del Interior.

b) Vigilancia y protección de bienes y establecimientos, cuando el número de vigilantes de seguridad que presten servicio en la provincia sea superior a treinta y la duración del servicio, con arreglo al contrato o a las prórrogas de éste, sea igual o superior a un año.

3. Las empresas de seguridad autorizadas para la prestación de actividades o servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión Europea de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, que hayan sido reconocidas en España con arreglo al procedimiento previsto en este real decreto, y que pretendan ejercer tales actividades o servicios en España con carácter permanente, deberán abrir delegaciones, sucursales, filiales o agencias en España.

Dichas delegaciones, sucursales, filiales o agencias deberán cumplir los requisitos previstos en el apartado 1 de este artículo y disponer de las medidas de seguridad previstas en este reglamento para las empresas de seguridad.

Artículo 18. *Características de los vehículos.*

Los vehículos utilizados por las empresas de seguridad habrán de reunir las características a que se refiere el artículo 1.d) de este Reglamento, no pudiendo disponer de lanza-destellos o sistemas acústicos destinados a obtener preferencia de paso a efectos de circulación vial.

Artículo 19. *Libros-registros.*

1. Las empresas de seguridad llevarán obligatoriamente los siguientes libros-registro:

a) Las empresas que estén obligadas a tener sistema de seguridad instalado, libro-catálogo de medidas de seguridad.

b) Libro-registro de comunicaciones a las Fuerzas y Cuerpos de Seguridad, en el que se anotarán cuantas realicen sobre aspectos relacionados con la seguridad ciudadana, fecha de cada comunicación, órgano al que se dirigió e indicación de su contenido.

2. El formato de los reseñados libros-registros se ajustará a las normas que respectivamente apruebe el Ministerio del Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

3. Tanto los libros-registro de carácter general como los específicos que se determinan en este Reglamento para cada actividad se llevarán en la sede principal de la empresa y en sus delegaciones o sucursales, debiendo estar siempre a disposición de los miembros del Cuerpo Nacional de Policía y de la Policía Autónoma correspondiente, encargados de su control.

4. En ausencia del director, administrador o jefe de seguridad, los libros-registro indicados se facilitarán por el personal presente en la empresa, que habrá de estar designado al efecto, durante las inspecciones que realicen los miembros de los citados Cuerpos o Policías.

Artículo 20. *Contratos de servicio.*

1. Las empresas de seguridad comunicarán con una antelación mínima de tres días, de forma individualizada para cada servicio, la iniciación del mismo, con indicación del lugar de prestación, la clase de actividad, la persona física o jurídica contratante y su domicilio, así como la duración prevista de la vigencia del contrato.

La referida comunicación de los contratos se efectuará por cualquier medio que permita dejar constancia de ello, en la comisaría provincial o local de policía del lugar donde se celebre el contrato, o, en los lugares en que éstas no existan, en los cuarteles o puestos de la Guardia Civil, que la transmitirán o remitirán con carácter urgente a la comisaría correspondiente al lugar en que haya de prestarse el servicio ; pudiendo efectuarse en cualquier caso, en los respectivos servicios o inspecciones de guardia.

Las modificaciones de los contratos se comunicarán, en la misma forma y plazos indicados, ante las dependencias policiales mencionadas.

El formato de los contratos y de las comunicaciones se ajustará a las normas y modelos que se establezcan por el Ministerio del Interior, sin perjuicio de la posibilidad de adición en los contratos, de pactos complementarios para aspectos no regulados en el presente Reglamento.

En cualquier caso, los contratos permanecerán en las sedes de las empresas de seguridad a disposición de los órganos de las Fuerzas y Cuerpos de Seguridad competentes en materia de inspección y control, durante un plazo de cinco años desde la finalización del servicio objeto del contrato.

2. En aquellos supuestos en que los contratos se concierten con Administraciones públicas o se encuentren en tramitación ante órganos de las mismas, no siendo posible que estén formalizados antes del inicio del servicio, las empresas de seguridad deberán aportar, en su caso, con la antelación indicada en el apartado anterior, copia autorizada o declaración de la empresa de la oferta formulada, para conocimiento de las circunstancias a que se refieren las cláusulas por los órganos encargados de la inspección y control, sin perjuicio de

comunicar en el formato establecido los datos del contrato una vez formalizado el mismo, el cual deberá quedar en la sede de la empresa a disposición de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

3. Cuando circunstancias excepcionales de robo, incendio, daños, catástrofes, conflictos sociales, averías de los sistemas de seguridad u otras causas de análoga gravedad o de extraordinaria urgencia, hicieran necesaria la prestación inmediata de servicio cuya organización previa hubiera sido objetivamente imposible, se comunicarán por el procedimiento más rápido disponible, antes de comenzar la prestación de los servicios, los datos enumerados en el párrafo primero del apartado 1 de este artículo a la dependencia policial correspondiente, indicando las causas determinantes de la urgencia, y quedando obligada la empresa a formalizar el contrato dentro de las setenta y dos horas siguientes a la iniciación del servicio, debiendo permanecer el contrato en la sede de la empresa a disposición de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

Los servicios de seguridad a que se refiere el párrafo anterior podrán ser prestados con armas, dando cuenta a la dependencia policial competente, cuando los supuestos descritos se produzcan en establecimientos obligados a tener medidas de seguridad que resulten anuladas por las circunstancias expuestas, o por otras, con grave riesgo para la integridad de los bienes protegidos y teniendo en cuenta la cuantía e importancia de éstos.

Artículo 21. *Contratos con defectos.*

Cuando la comunicación, el contrato o la oferta de servicios de las empresas de seguridad no se ajusten a las exigencias prevenidas, la Subdelegación del Gobierno -que podrá delegar en la correspondiente Jefatura Superior o Comisaría Provincial de Policía- les notificará las deficiencias, con carácter urgente, a efectos de que puedan ser subsanadas en los cinco días hábiles siguientes, con apercibimiento de que, de no hacerlo en el plazo indicado, los citados documentos se archivarán sin más trámite, no pudiendo comenzar la prestación del servicio, o continuarla si ya hubiese comenzado.

Artículo 22. *Suspensión de servicios.*

(Anulado)

Sección 2.ª Empresas inscritas para actividades de vigilancia, protección de personas y bienes, depósito, transporte y distribución de objetos valiosos, explosivos u objetos peligrosos

Artículo 23. *Adecuación de los servicios a los riesgos.*

Las empresas inscritas y autorizadas para el desarrollo de las actividades a que se refieren los párrafos a), b), c) y d) del artículo 1 de este Reglamento, antes de formalizar la contratación de un servicio de seguridad, deberán determinar bajo su responsabilidad la adecuación del servicio a prestar respecto a la seguridad de las personas y bienes protegidos, así como la del personal de seguridad que haya de prestar el servicio, teniendo en cuenta los riesgos a cubrir, formulando, en consecuencia, por escrito, las indicaciones procedentes.

Artículo 24. *Comunicación entre la sede de la empresa y el personal de seguridad.*

Las empresas deberán asegurar la comunicación entre su sede y el personal que desempeñe los siguientes servicios:

a) Vigilancia y protección de polígonos industriales o urbanizaciones.
b) Transporte y distribución de objetos valiosos o peligrosos.
c) Custodia de llaves en vehículos, en servicios de respuesta a alarmas.
d) Aquellos otros que, por sus características, se determinen por el Gobierno Civil de la provincia.

Artículo 25. *Armeros.*

1. En los lugares en que se preste servicio de vigilantes de seguridad con armas o de protección de personas determinadas, salvo en aquellos supuestos en que la duración del servicio no exceda de un mes, deberán existir armeros que habrán de estar aprobados por el Gobierno Civil de la provincia, previo informe de la correspondiente Intervención de Armas y Explosivos de la Guardia Civil, una vez comprobado que se cumplen las medidas de seguridad determinadas por la Dirección General de la Guardia Civil.

2. En dichos lugares, deberá existir un libro-registro de entrada y salida de armas, concebido de forma que sea posible su tratamiento y archivo mecanizado e informatizado, en el que se anotarán, en cada relevo que se produzca en el servicio, las armas depositadas, las armas que portan los vigilantes, y los restantes datos que se determinen en el correspondiente modelo.

3. En el domicilio social de las empresas de seguridad o en el de sus delegaciones o sucursales, según proceda, deberá estar depositada una llave de tales armeros.

4. Cuando se trate de los servicios especiales determinados en el artículo 82.2 de este Reglamento, la utilización del armero podrá sustituirse por el uso de la caja fuerte del local, custodiando el arma en una caja metálica cerrada con llave. La llave de esta caja metálica deberá estar en posesión del vigilante, y una copia depositada en el domicilio de la empresa de seguridad o en el de su delegación o sucursal.

Artículo 26. *Armas reglamentarias.*

1. Las armas reglamentarias que han de portar y utilizar los vigilantes de seguridad, escoltas privados y guardas particulares del campo, en el ejercicio de sus funciones, se adquirirán por las empresas y serán de su propiedad.

2. Para la tenencia legal de dichas armas, en número que no podrá exceder del que permitan las licencias obtenidas por el personal con arreglo al Reglamento de Armas, las empresas de seguridad habrán de solicitar y necesitarán obtener de los órganos correspondientes de la Dirección General de la Guardia Civil las guías de pertenencia de dichas armas.

3. Además de las armas que posean para la prestación de los servicios, las empresas de seguridad habrán de disponer de armas en número equivalente al 10 por 100 del de vigilantes de seguridad, al objeto de que éstos puedan realizar los ejercicios obligatorios de tiro. La Dirección General de la Guardia Civil comunicará a la de la Policía, y, en su caso, a la Policía de la correspondiente Comunidad Autónoma, el número y clases de armas que las empresas tengan en cada uno de sus locales.

4. El personal a que se refiere el apartado 1 del presente artículo realizará los ejercicios obligatorios de tiro en la fecha que se determine por las empresas de seguridad, bajo la supervisión de la Guardia Civil, de acuerdo con las instrucciones que imparta la Dirección General de dicho Cuerpo.

5. En las galerías de tiro en que se lleven a cabo los ejercicios, que habrán de encontrarse autorizadas conforme a lo previsto en el Reglamento de Armas, tanto si son propias como si son ajenas a las empresas de seguridad, los vigilantes de seguridad, escoltas privados y demás personal de seguridad privada habrán de realizar las prácticas de manejo y perfeccionamiento en el uso de armas, siempre ante la presencia y bajo la dirección del jefe de seguridad o de un instructor de tiro, ambos de competencia acreditada.

Sección 3.ª Protección de personas

Artículo 27. *Personas y empresas autorizadas.*

La actividad de protección de personas podrá ser desarrollada únicamente por escoltas privados integrados en empresas de seguridad, inscritas para el ejercicio de dicha actividad, y que habrán de obtener previamente autorización específica para cada contratación de servicio de protección, de acuerdo con lo dispuesto en los artículos siguientes.

Artículo 28. *Solicitud, tramitación y resolución.*

1. Los servicios de protección deberán ser solicitados, directamente por la persona interesada o a través de la empresa de seguridad que se pretenda encargar de prestarlos, ya sean en favor del propio interesado o de las personas que tenga bajo su guarda o custodia o de cuya seguridad fuera responsable.

2. El procedimiento se tramitará con carácter urgente, y en el mismo habrá de obtenerse el informe de la Dirección General de la Guardia Civil, cuando sea procedente, teniendo en cuenta los lugares en que haya de realizarse principalmente la actividad.

En la solicitud, que se dirigirá al Director general de la Policía, se harán constar los riesgos concretos de las personas a proteger, valorando su gravedad y probabilidad y acompañando cuantos datos o informes se consideren pertinentes para justificar la necesidad del servicio. Asimismo, cuando la autorización se solicite personalmente, se expresará en la solicitud la empresa de seguridad a la que se pretenda encargar de prestarlo.

3. La Dirección General de la Policía, considerando la naturaleza del riesgo, su gravedad y probabilidad, determinará si es necesaria la prestación del servicio de protección o si, por el contrario, es suficiente la adopción de medidas de autoprotección. Los servicios de protección personal habrán de ser autorizados, expresa e individualizadamente y con carácter excepcional, cuando, a la vista de las circunstancias expresadas resulten imprescindibles, y no puedan cubrirse por otros medios.

4. La resolución en que se acuerde la concesión o denegación de la autorización, que habrá de ser motivada, determinará el plazo de vigencia de la misma, podrá incorporar condicionamientos sobre su forma de prestación, concretará si ha de ser prestado por uno o más escoltas privados con las armas correspondientes, y se comunicará al interesado y a la empresa de seguridad.

Artículo 29. *Autorización provisional.*

Cuando con base en la solicitud e información presentada con arreglo al apartado 1 del artículo 28 resultara necesario, teniendo en cuenta las circunstancias y urgencia del caso, podrá concederse con carácter inmediato una autorización provisional para la prestación de servicios de protección personal, por el tiempo imprescindible hasta que se pueda adoptar la resolución definitiva.

Artículo 30. *Prestación y finalización del servicio.*

1. La empresa de seguridad encargada comunicará a la Dirección General de la Policía la composición del personal de la escolta, así como sus variaciones tan pronto como se produzcan, informando en su caso de los escoltas relevados, de los que les sustituyan y de las causas de la sustitución.

2. **(Derogado)**

3. Los servicios de protección de personas podrán ser prorrogados, a instancia del solicitante, cuando lo justifiquen las circunstancias que concurran.

4. La empresa de seguridad deberá comunicar a la Dirección General de la Policía la finalización del servicio, así como sus causas, en el plazo de las cuarenta y ocho horas siguientes al momento de producirse aquélla.

5. Simultáneamente a la notificación de las autorizaciones que conceda, la Dirección General de la Policía comunicará a las unidades correspondientes de las Fuerzas y Cuerpos de Seguridad del Estado las autorizaciones concedidas, los datos de las personas protegidas y de los escoltas encargados de los servicios, así como su fecha de iniciación y finalización.

Sección 4.ª Depósito y custodia de objetos valiosos o peligrosos y explosivos

Artículo 31. *Particularidades de estos servicios.*

1. En los contratos en que se concierte la prestación de servicios de depósito y custodia habrá de constar la naturaleza de los objetos que hayan de ser depositados o custodiados y, en su caso, clasificados, así como una valoración de los mismos.

2. Las empresas dedicadas a la prestación de estos servicios llevarán un libro-registro de depósitos, cuyo formato se ajustará a las normas que se aprueben por el Ministerio del Interior.

Sección 5.ª Transporte y distribución de objetos valiosos o peligrosos y explosivos

Artículo 32. *Vehículos.*

1. La prestación de los servicios de transporte y distribución de objetos valiosos o peligrosos habrá de efectuarse en vehículos blindados de las características que se determinen por el Ministerio de Justicia e Interior, cuando las cantidades, el valor o la peligrosidad de lo transportado superen los límites o reúnan las características que asimismo establezca dicho Ministerio, sin perjuicio de las competencias que corresponden al Ministerio de Industria y Energía.

Cuando las características o tamaño de los objetos, especificados por Orden del Ministerio de Justicia e Interior impidan o hagan innecesario su transporte en vehículos blindados, éste se podrá realizar en otros vehículos, contando con la debida protección en cada caso, determinada con carácter general en dicha Orden o, para cada caso concreto, por el correspondiente Gobierno Civil.

Los viajantes de joyería solamente podrán llevar consigo reproducciones de joyas u objetos preciosos cuya venta promocionen, o las piezas originales, cuando su valor en conjunto no exceda de la cantidad que determine el Ministerio de Justicia e Interior.

2. Las características de los vehículos de transporte y distribución de explosivos se determinarán teniendo en cuenta lo dispuesto en el Reglamento de Transporte de Mercancías Peligrosas (TPC), para dichas materias.

Artículo 33. *Dotación y funciones.*

1. La dotación de cada vehículo blindado estará integrada, como mínimo, por tres vigilantes de seguridad, uno de los cuales realizará exclusivamente la función de conductor.

2. Durante las operaciones de transporte, carga y descarga, el conductor se ocupará del control de los dispositivos de apertura y comunicación del vehículo, y no podrá abandonarlo; manteniendo en todo momento el motor en marcha cuando se encuentre en vías urbanas o lugares abiertos. Las labores de carga y descarga las efectuará otro vigilante, encargándose de su protección durante la operación el tercer miembro de la dotación, que portará al efecto el arma determinada de acuerdo con lo dispuesto en el artículo 86 de este Reglamento.

3. La dotación y las funciones de los vigilantes de cada vehículo de transporte y distribución de explosivos se determinarán con arreglo a lo que disponga el Reglamento de Explosivos, aprobado por el Real Decreto 230/1998, de 16 de febrero.

Artículo 34. *Hoja de ruta.*

1. Las operaciones de recogida y entrega que realice cada vehículo se consignarán diariamente en una hoja de ruta, que podrá estar informatizada en papel continuo, y se archivará por orden numérico en formato de libro, o en cualquier otro que respete su secuencia, conteniendo los datos que determine el Ministerio del Interior.

Los funcionarios policiales encargados de la inspección podrán requerir la exhibición de las hojas de ruta en cualquier momento, durante el desarrollo de la actividad, debiendo conservarse aquéllas, o el soporte magnético o digital en el que se consignó la información, durante cinco años, en la sede de la empresa o de las correspondientes delegaciones, o en

locales de empresas especializadas en el archivo de documentación -en este caso con conocimiento del servicio policial correspondiente.

2. En el caso de transporte y distribución de explosivos, la hoja de ruta será sustituida por la documentación análoga que, para la circulación de dichas sustancias, se establece en el Reglamento de Explosivos y normativa complementaria.

Artículo 35. *Libro-registro.*

Las empresas dedicadas al transporte y distribución de títulos-valores llevarán un libro-registro, cuyo formato se ajustará a las normas que se aprueben por el Ministerio del Interior.

Artículo 36. *Comunicación previa del transporte.*

Siempre que la cuantía e importancia de los fondos, valores u objetos exceda de la cantidad o la peligrosidad de los objetos reúna las características que determine el Ministerio de Justicia e Interior, el transporte deberá ser comunicado a la dependencia correspondiente de la Dirección General de la Policía, si es urbano, y a la de la Dirección General de la Guardia Civil, si es interurbano, con veinticuatro horas de antelación al comienzo de la realización del servicio.

Artículo 37. *Otros medios de transporte.*

1. El transporte de fondos, valores y otros bienes u objetos valiosos se podrá realizar por vía aérea, utilizando los servicios ordinarios de las compañías aéreas o aparatos de vuelo propios.

2. Cuando en el aeropuerto existan caja fuerte y servicios especiales de seguridad, se podrá encargar a dichos servicios de las operaciones de carga y descarga de los bienes u objetos valiosos, con las precauciones que se señalan en los apartados siguientes.

3. Cuando en el aeropuerto no exista caja fuerte o servicios de seguridad, los vehículos blindados de las empresas de seguridad, previa facturación en la zona de seguridad de las terminales de carga, se dirigirán, con su dotación de vigilantes de seguridad y armamento reglamentario, hasta el punto desde el que se pueda realizar directamente la carga de bultos y valijas en la aeronave, debiendo permanecer en este mismo lugar hasta que se produzca el cierre y precinto de la bodega.

4. En la descarga se adoptarán similares medidas de seguridad, debiendo los vigilantes de dotación estar presentes con el vehículo blindado en el momento de la apertura de la bodega.

5. A los efectos de cumplimentar dichas obligaciones, la dirección de cada aeropuerto facilitará a las empresas de seguridad responsables del transporte las acreditaciones y permisos oportunos.

6. Análogas reglas y precauciones se seguirán para el transporte de fondos, valores y otros bienes u objetos valiosos por vía marítima.

Artículo 38. *Transporte de explosivos y objetos peligrosos.*

1. Las empresas de seguridad pueden dedicarse al transporte o a la protección del transporte de explosivos o de otras sustancias u objetos peligrosos, lo que habrá de realizarse cumpliendo lo prevenido en el presente Reglamento, en los Reglamentos de Armas y de Explosivos, y lo que se establezca al respecto en la normativa vigente, aplicable al transporte de mercancías peligrosas, debiendo ser adecuado el servicio de seguridad al riesgo a cubrir.

2. En el caso de transporte de explosivos, estos servicios se realizarán con vigilantes de seguridad, que estén en posesión de la habilitación especial prevenida al efecto en el presente Reglamento, debiendo los vehículos estar autorizados para tal finalidad por la Administración Pública competente.

Sección 6.ª Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad

Artículo 39. *Ambito material.*

1. Únicamente las empresas autorizadas podrán realizar las operaciones de instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad electrónica contra robo e intrusión y contra incendios que se conecten a centrales receptoras de alarmas.

A efectos de su instalación y mantenimiento, tendrán la misma consideración que las centrales de alarmas los denominados centros de control o de video vigilancia, entendiendo por tales los lugares donde se centralizan los sistemas de seguridad y vigilancia de un edificio o establecimiento y que obligatoriamente deban estar controlados por personal de seguridad privada.

2. Queda prohibida la instalación de marcadores automáticos programados para transmitir alarmas directamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 40. *Aprobación de material.*

1. Los medios materiales y técnicos, aparatos de alarma y dispositivos de seguridad que instalen y utilicen estas empresas, habrán de encontrarse debidamente aprobados con arreglo a las normas que se establezcan, impidiendo que los sistemas de seguridad instalados causen daños o molestias a terceros.

2. Los dispositivos exteriores, tales como cajas de avisadores acústicos u ópticos, deberán incorporar el teléfono de contacto desde el que se pueda adoptar la decisión adecuada, y el nombre y teléfono de la empresa que realice su mantenimiento.

Artículo 41. *Personal de las empresas.*

1. Las actividades de las empresas se realizarán por el personal que posea la titulación exigida.

2. En caso de sustitución del personal titulado, deberá comunicarse a la Dirección General de la Policía u órgano correspondiente de la Comunidad Autónoma competente, adjuntando copia compulsada del título del nuevo empleado incorporado, o el propio título, con copia, a fin de que, una vez compulsada con el original, sea devuelto éste a la empresa.

Artículo 42. *Certificado de instalación y conexión a central de alarmas.*

1. Las instalaciones de sistemas de seguridad deberán ajustarse a lo dispuesto en la normativa reguladora de las instalaciones eléctricas en lo que les sea de aplicación.

2. En los supuestos de instalación de medidas de seguridad obligatorias en empresas o entidades privadas que carezcan de Departamento de Seguridad, o cuando tales empresas o entidades se vayan a conectar a centrales de alarmas, la instalación deberá ser precedida de la elaboración y entrega al usuario de un proyecto de instalación, con niveles de cobertura adecuados a las características arquitectónicas del recinto y del riesgo a cubrir, de acuerdo con los criterios técnicos de la propia empresa instaladora y, eventualmente, los de la dependencia policial competente, todo ello con objeto de alcanzar el máximo grado posible de eficacia del sistema, de fiabilidad en la verificación de las alarmas, de colaboración del usuario, y de evitación de falsas alarmas.

3. Una vez realizada la instalación, las empresas instaladoras efectuarán las comprobaciones necesarias para asegurarse de que se cumple su finalidad preventiva y protectora, y de que es conforme con el proyecto contratado y con las disposiciones reguladoras de la materia, debiendo entregar a la entidad o establecimiento usuarios un certificado en el que conste el resultado positivo de las comprobaciones efectuadas.

4. Las instalaciones de seguridad habrán de reunir las características que se determinen por Orden del Ministro del Interior, y el certificado a que se refiere el apartado anterior deberá emitirse por ambas empresas, conjunta o separadamente, de forma que se garantice su funcionalidad global.

Artículo 43. *Revisiones.*

1. Los contratos de instalación de aparatos, dispositivos y sistemas de seguridad, en los supuestos en que la instalación sea obligatoria o cuando se conecten con una central de alarmas, comprenderán el mantenimiento de la instalación en estado operativo, con revisiones preventivas cada trimestre, no debiendo, en ningún caso, transcurrir más de cuatro meses entre dos revisiones sucesivas. En el momento de suscribir el contrato de instalación o en otro posterior, la entidad titular de la instalación podrá, sin embargo, asumir por sí misma o contratar el servicio de mantenimiento y la realización de revisiones trimestrales con otra empresa de seguridad.

2. Cuando las instalaciones permitan la comprobación del estado y del funcionamiento de cada uno de los elementos del sistema desde la central de alarmas, las revisiones preventivas tendrán una periodicidad anual, no pudiendo transcurrir más de catorce meses entre dos sucesivas.

3. Las revisiones preventivas podrán ser realizadas directamente por las entidades titulares de las instalaciones, cuando dispongan del personal con la cualificación requerida, y de los medios técnicos necesarios.

4. Las empresas de seguridad dedicadas a esta actividad y las titulares de las instalaciones llevarán libros-registros de revisiones, cuyos modelos se ajusten a las normas que se aprueben por el Ministerio de Justicia e Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

Artículo 44. *Averías.*

Para el adecuado cumplimiento de lo dispuesto en el artículo anterior, las empresas de instalación y mantenimiento deberán disponer del servicio técnico adecuado que permita atender debidamente las averías de los sistemas de seguridad de cuyo mantenimiento se hayan responsabilizado, incluso en días festivos, en el plazo de veinticuatro horas siguientes al momento en que hayan sido requeridas al efecto. De las características de este servicio y de sus modificaciones, las empresas informarán oportunamente a la Dirección General de la Policía.

Artículo 45. *Manuales del sistema.*

1. Las empresas facilitarán al usuario un manual de la instalación que describirá, mediante planos y explicaciones complementarias, la distribución de las canalizaciones, el cableado, las conexiones de los equipos, las líneas eléctricas y de alarma, así como el detalle de los elementos y aparatos instalados y soportes utilizados.

2. Igualmente, entregarán un manual de uso del sistema y de su mantenimiento, que incluirá el detalle de la función que cumple cada dispositivo y la forma de usarlos separadamente o en su conjunto, así como el mantenimiento preventivo y correctivo de los aparatos o dispositivos mecánicos o electrónicos instalados, con evaluación de su vida útil, y una relación de las averías más frecuentes y de los ajustes necesarios para el buen funcionamiento del sistema.

3. En el caso de que un sistema de seguridad instalado sufra alguna variación posterior que modifique sustancialmente el originario, en todo o en parte, la empresa instaladora o, en su caso, la de mantenimiento, vendrá obligada a confeccionar nuevos manuales de instalación, uso y mantenimiento. Asimismo, la empresa instaladora deberá comunicarlo también a la central de alarmas y certificar, en la forma que se establece en el artículo 42, el resultado de las comprobaciones.

Sección 7.ª Centrales de alarmas

Artículo 46. *Requisitos de conexión.*

Para conectar aparatos, dispositivos o sistemas de seguridad a centrales de alarmas será preciso que la realización de la instalación haya sido efectuada por una empresa de

seguridad inscrita en el registro correspondiente y se ajuste a lo dispuesto en los artículos 40, 42 y 43 de este Reglamento.

Artículo 47. *Información al usuario.*

Antes de efectuar la conexión, las empresas explotadoras de centrales de alarmas están obligadas a instruir al usuario del funcionamiento del servicio, informándole de las características técnicas y funcionales del sistema y de las responsabilidades que lleva consigo su incorporación al mismo.

Artículo 48. *Funcionamiento.*

1. La central de alarmas deberá estar atendida permanentemente por los operadores necesarios para la prestación de los servicios, que no podrán, en ningún caso, ser menos de dos, y que se encargarán del funcionamiento de los receptores y de la transmisión de las alarmas que reciban.

2. Cuando se produzca una alarma, las centrales deberán proceder de inmediato a su verificación con los medios técnicos y humanos de que dispongan, y comunicar seguidamente al servicio policial correspondiente las alarmas reales producidas.

Artículo 49. *Servicio de custodia de llaves.*

1. Las empresas explotadoras de centrales de alarmas podrán contratar, complementariamente, con los titulares de los recintos conectados, un servicio de custodia de llaves, de verificación de alarmas mediante desplazamiento a los propios recintos, y de respuesta a las mismas, en las condiciones que se determinen por el Ministerio del Interior, a cuyo efecto deberán disponer del armero o caja fuerte exigidos con arreglo a lo dispuesto en el artículo 25 de este Reglamento.

Las empresas industriales, comerciales o de servicios que estén autorizadas a disponer de central de alarmas, dedicada exclusivamente a su propia seguridad, podrán contratar los mismos servicios con una empresa de seguridad autorizada para vigilancia y protección.

2. Los servicios de verificación personal de las alarmas y de respuesta a las mismas se realizarán, en todo caso, por medio de vigilantes de seguridad, y consistirán, respectivamente, en la inspección del local o locales, y en el traslado de las llaves del inmueble del que procediere cada alarma, todo ello a fin de facilitar a los miembros de las Fuerzas y Cuerpos de Seguridad información sobre posible comisión de hechos delictivos y su acceso al referido inmueble.

A los efectos antes indicados, la inspección del interior de los inmuebles por parte de los vigilantes de seguridad deberá estar expresamente autorizada por los titulares de aquéllos, consignándose por escrito en el correspondiente contrato de prestación de servicios.

3. Cuando por el número de servicios de custodia de llaves o por la distancia entre los inmuebles resultare conveniente para la empresa y para los servicios policiales, aquélla podrá disponer, previa autorización de éstos, que las llaves sean custodiadas por vigilantes de seguridad sin armas en un automóvil, conectado por radio-teléfono con la central de alarmas. En este supuesto, las llaves habrán de estar codificadas, debiendo ser los códigos desconocidos por el vigilante que las porte y variados periódicamente.

4. Para los servicios a que se refieren los dos apartados anteriores, las empresas de seguridad explotadoras de centrales de alarmas podrán contar con vigilantes de seguridad, sin necesidad de estar inscritas y autorizadas para la actividad de vigilancia y protección de bienes, o bien subcontratar tal servicio con una empresa de esta especialidad.

Artículo 50. *Desconexión por falsas alarmas.*

1. En los supuestos de conexión de aparatos, dispositivos o sistemas de seguridad con una central de alarmas, con independencia de la responsabilidad y sanciones a que hubiere lugar, cuando el sistema origine dos o más falsas alarmas en el plazo de un mes, el Delegado del Gobierno, que podrá delegar en el Jefe Superior o Comisario Provincial de Policía, requerirá al titular de los bienes protegidos, a través de la dependencia policial que corresponda, para que proceda, a la mayor brevedad posible, a la subsanación de las deficiencias que dan lugar a las falsas alarmas.

2. A los efectos del presente Reglamento, se considera falsa toda alarma que no esté determinada por hechos susceptibles de producir la intervención policial. No tendrá tal consideración la mera repetición de una señal de alarma causada por una misma avería dentro de las veinticuatro horas siguientes al momento en que ésta se haya producido.

3. En caso de incumplimiento del requerimiento, se ordenará a la empresa explotadora de la central de alarma que efectúe la inmediata desconexión del sistema con la propia central, por el plazo que se estime conveniente, que podrá tener hasta un año de duración, salvo que se subsanaran en plazo más breve las deficiencias que den lugar a la desconexión, siendo la tercera desconexión de carácter definitivo, y requiriéndose para una nueva conexión el cumplimiento de lo prevenido en el artículo 42 de este Reglamento. Durante el tiempo de desconexión, el titular de la propiedad o bien protegido deberá silenciar las sirenas interiores y exteriores del sistema de seguridad.

4. Durante el tiempo que permanezca desconectado como consecuencia de ello un sistema de seguridad, su titular no podrá concertar el servicio de centralización de alarmas con ninguna empresa de seguridad.

5. Sin perjuicio de la apertura del correspondiente expediente, no se procederá a desconectar el sistema de seguridad cuando su titular estuviere obligado, con arreglo a lo dispuesto por este Reglamento, a contar con dicha medida de seguridad.

6. Cuando el titular de la propiedad o bien protegido por el sistema de seguridad no tenga contratado el servicio de centralización de alarmas y la realizare por sí mismo, se aplicará lo dispuesto en el apartado 1 de este artículo, correspondiéndole, en todo caso, la obligación de silenciar las sirenas interiores y exteriores que posea dicho sistema de seguridad, sin perjuicio de la responsabilidad en que hubiera podido incurrir.

Artículo 51. *Libros registros.*

1. Las empresas de explotación de centrales de alarma llevarán un libro-registro de alarmas, cuyo modelo se ajuste a las normas que apruebe el Ministerio del Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

2. Las centrales de alarmas que tengan contratado servicio de custodia de llaves indicarán en el libro-registro de contratos cuáles de éstos incluyen aquel servicio.

TITULO II

Personal de seguridad

CAPITULO I

Habilitación y formación

Sección 1.ª Requisitos

Artículo 52. *Disposiciones comunes.*

1. El personal de seguridad privada estará integrado por: los vigilantes de seguridad, los vigilantes de explosivos, los jefes de seguridad, los directores de seguridad, los escoltas privados, los guardas particulares del campo, los guardas de caza, los guardapescas marítimos y los detectives privados.

2. A los efectos de habilitación y formación, se considerarán:

a) Los escoltas privados y los vigilantes de explosivos y sustancias peligrosas como especialidades de los vigilantes de seguridad.

b) Los guardas de caza y los guardapescas marítimos como especialidades de los guardas particulares del campo.

3. Para el desarrollo de sus respectivas funciones, el personal de seguridad privada habrá de obtener previamente la correspondiente habilitación o reconocimiento del Ministerio

del Interior, con el carácter de autorización administrativa, en expediente que se instruirá a instancia de los propios interesados.

4. La habilitación o reconocimiento se documentará mediante la correspondiente tarjeta de identidad profesional, cuyas características serán determinadas por el Ministerio del Interior.

5. Los vigilantes de seguridad y los guardas particulares del campo en sus distintas modalidades habrán de disponer, además, de una cartilla profesional y de una cartilla de tiro con las características y anotaciones que se determinen por el Ministerio del Interior. La cartilla profesional y la cartilla de tiro de los vigilantes de seguridad y de los guardas particulares del campo que estén integrados en empresas de seguridad deberán permanecer depositadas en la sede de la empresa de seguridad en la que presten sus servicios.

6. De la obligación de disponer de cartilla de tiro estarán exonerados los guardapescas marítimos que habitualmente presten su servicio sin armas.

7. La habilitación o el reconocimiento para el ejercicio de la profesión de detective privado requerirá la inscripción en el registro específico regulado en el presente reglamento.

Artículo 53. *Requisitos generales.*

Para la habilitación del personal y en todo momento para la prestación de servicios de seguridad privada, el personal habrá de reunir los siguientes requisitos generales:

a) Ser mayor de edad.

b) Tener la nacionalidad de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

c) Poseer la aptitud física y la capacidad psíquica necesarias para el ejercicio de las respectivas funciones sin padecer enfermedad que impida el ejercicio de las mismas.

d) Carecer de antecedentes penales.

e) No haber sido condenado por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud.

f) No haber sido sancionado en los dos o cuatro años anteriores, respectivamente, por infracción grave o muy grave en materia de seguridad.

g) No haber sido separado del servicio en las Fuerzas Armadas o en las Fuerzas y Cuerpos de Seguridad.

h) No haber ejercido funciones de control de las entidades, servicios o actuaciones de seguridad, vigilancia o investigación privadas, ni de su personal o medios, como miembro de las Fuerzas y Cuerpos de Seguridad en los dos años anteriores a la solicitud.

i) Superar las pruebas que acrediten los conocimientos y la capacitación necesarios para el ejercicio de las respectivas funciones.

Artículo 54. *Requisitos específicos.*

1. Además de los requisitos generales establecidos en el artículo anterior, el personal de seguridad privada habrá de reunir, para su habilitación, los determinados en el presente artículo, en función de su especialidad.

2. Vigilantes de seguridad y guardas particulares del campo en cualquiera de sus especialidades:

a) No haber cumplido los cincuenta y cinco años de edad.

b) Estar en posesión del título de Graduado en Educación Secundaria Obligatoria, de Técnico, u otros equivalentes a efectos profesionales, o superiores.

c) Los requisitos necesarios para poder portar y utilizar armas de fuego, a tenor de lo dispuesto al efecto en el vigente Reglamento de Armas.

3. Escoltas privados: además de los requisitos específicos de los vigilantes de seguridad, habrán de tener una estatura mínima de 1.70 metros los hombres, y de 1.65 metros las mujeres.

4. Jefes de seguridad y directores de seguridad: estar en posesión del título de Bachiller, de Técnico Superior, de Técnico en las profesiones que se determinen, u otros equivalentes a efectos profesionales, o superiores.

5. Detectives privados:

a) Estar en posesión del título de Bachiller, de Técnico Superior, de Técnico en las profesiones que se determinen, u otros equivalentes a efectos profesionales, o superiores.

b) Estar en posesión de diploma de detective privado, reconocido a estos efectos en la forma que se determine por Orden del Ministerio del Interior y obtenido después de cursar las enseñanzas programadas y de superar las correspondientes pruebas.

Artículo 55. *Fecha y acreditación.*

Los requisitos establecidos en los dos artículos anteriores deberán reunirse en la fecha de terminación del plazo de presentación de la solicitud para la participación en las pruebas a que se refiere el artículo 58 de este Reglamento ante la Secretaría de Estado de Interior, y se acreditarán en la forma que se determine en las correspondientes convocatorias.

Artículo 55 bis. *Requisitos y procedimiento para el reconocimiento.*

1. Los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, cuya habilitación o cualificación profesional haya sido obtenida en alguno de dichos Estados para el desempeño de las funciones de seguridad privada en el mismo, podrán desempeñar actividades o prestar servicios de seguridad privada en España, siempre que, previa comprobación del Ministerio del Interior, se acredite que cumplen los siguientes requisitos:

a) Poseer alguna titulación, habilitación o certificación expedida por las autoridades competentes de cualquiera de dichos Estados, que les autorice para el ejercicio de funciones de seguridad privada en el mismo.

b) Acreditar los conocimientos, formación y aptitudes equivalentes a los exigidos en España para el ejercicio de las profesiones relacionadas con la seguridad privada. c) Tener conocimientos de lengua castellana suficientes para el normal desempeño de las funciones de seguridad privada. d) Los previstos en las letras a), d), e), f), g) y h) del artículo 53.

2. A efectos del reconocimiento que corresponde efectuar al Ministerio del Interior, se tendrá en cuenta lo previsto en la normativa sobre reconocimiento de cualificaciones profesionales.

3. La carencia o insuficiencia de conocimientos o aptitudes necesarios para el ejercicio de las actividades de seguridad privada en España de los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, podrá suplirse por aplicación de las medidas compensatorias previstas en la normativa reseñada en el párrafo anterior. 4. Una vez efectuado el citado reconocimiento, el ejercicio de las funciones de seguridad privada se regirá por lo dispuesto en este reglamento y en la normativa que lo desarrolla.

Sección 2.ª Formación

Artículo 56. *Formación previa.*

1. Los vigilantes de seguridad y los guardas particulares del campo en sus distintas modalidades habrán de superar los módulos profesionales de formación teórico-práctica asociados al dominio de las competencias que la Ley les atribuye.

Los conocimientos, habilidades, destrezas y actitudes a alcanzar en dichos módulos, así como su duración serán determinados por el Ministerio de Justicia e Interior, previo informe favorable de los Ministerios de Educación y Ciencia, y de Trabajo y Seguridad Social, así como del Ministerio de Agricultura, Pesca y Alimentación respecto a los guardas particulares del campo, y del Ministerio de Industria y Energía respecto de los vigilantes de seguridad especialidad de explosivos y sustancias peligrosas.

2. Dichos módulos formativos los impartirán los centros de formación autorizados por la Secretaría de Estado de Seguridad, los cuales habrán de disponer de un cuadro de profesores debidamente acreditados para todas las materias comprendidas en el plan de estudios, y podrán impartir, en la modalidad de formación a distancia, las enseñanzas que se determinen, exceptuando en cualquier caso las de naturaleza técnico-profesional, instrumental, de contenido técnico-operativo y las prácticas de laboratorio y de tiro, que deberán impartirse necesariamente en la modalidad "de presencia" durante el tiempo que como mínimo determine el Ministerio del Interior.

Artículo 57. *Formación permanente.*

1. Al objeto de mantener al día el nivel de aptitud y conocimientos necesarios para el ejercicio de las funciones atribuidas al personal de seguridad privada, las empresas de seguridad, a través de los centros de formación autorizados, garantizarán la organización y asistencia de su personal de seguridad privada a cursos, adaptados a las distintas modalidades de personal, de actualización en las materias que hayan experimentado modificación o evolución sustancial, o en aquellas que resulte conveniente una mayor especialización.

2. Para los vigilantes de seguridad, los cursos de actualización o especialización tendrán una duración, como mínimo, de veinte horas lectivas; cada vigilante deberá cursar al menos uno por año, y se desarrollarán en la forma que determine el Ministerio del Interior.

Sección 3.ª Procedimiento de habilitación

Artículo 58. *Pruebas. Contenido.*

Los aspirantes que hayan superado el curso o cursos a que se refiere el artículo 56 solicitarán, por sí mismos o a través de un centro de formación autorizado, su participación en las pruebas oficiales de conocimientos y capacidad que para cada especialidad establezca el Ministerio del Interior, y que versarán sobre materias sociales, jurídicas y técnicas relacionadas con las respectivas funciones, así como, en su caso, sobre destreza en el manejo de armas de fuego.

Una vez superadas las pruebas, los órganos policiales correspondientes expedirán las oportunas habilitaciones.

Artículo 59. *Documentación.*

Con la solicitud, se presentarán los documentos que acrediten el cumplimiento de los requisitos generales y específicos determinados en los artículos 53 y 54.

Artículo 60. *Organo competente.*

Las tarjetas de identidad profesional, una vez superadas las pruebas, serán expedidas por el Director general de la Policía, salvo las de los guardas particulares del campo en sus distintas modalidades, que serán expedidas por el Director general de la Guardia Civil.

Artículo 61. *Licencias de armas.*

1. Para poder prestar servicios con armas, los vigilantes de seguridad y escoltas privados, así como los guardas particulares del campo habrán de obtener licencia C en la forma prevenida en el Reglamento de Armas.

2. Dicha licencia tendrá validez exclusivamente para la prestación del servicio de seguridad, en los supuestos determinados en el presente Reglamento; carecerá de validez cuando su titular no se encuentre realizando servicios; podrá ser suspendida temporalmente por falta de realización o por resultado negativo de los ejercicios de tiro regulados en el artículo 84 de este Reglamento; y quedará sin efecto al cesar aquél en el desempeño del puesto en razón del cual le hubiera sido concedida, cualquiera que fuere la causa del cese.

Artículo 62. *Habilitación múltiple.*

Sin perjuicio de las incompatibilidades prevenidas en la Ley y en el presente Reglamento, el personal de seguridad privada podrá obtener habilitación para más de una función o especialidad y poseer en consecuencia las correspondientes tarjetas de identidad profesional.

El personal de seguridad privada que ya se encuentre diplomado o habilitado como vigilante de seguridad o como guarda particular del campo, para la obtención de diplomas o de habilitaciones complementarias, únicamente necesitará recibir la formación y/o, en su caso, superar las pruebas correspondientes a los módulos de formación profesional que sean propios del nuevo diploma o habilitación que deseen obtener, excluyéndose en consecuencia los relativos a la formación o a la habilitación que anteriormente hubieran adquirido.

Asimismo, a efectos de las habilitaciones complementarias a que se refiere el párrafo anterior, al personal que ya se encuentre habilitado como vigilante de seguridad o como guarda particular del campo, no le será aplicable el requisito de no haber cumplido cuarenta, o, en su caso, cuarenta y cinco años de edad.

Artículo 63. *Habilitación de jefes de seguridad y de directores de seguridad.*

1. Para poder ser nombrados jefes de seguridad, los solicitantes deberán haber desempeñado puestos o funciones de seguridad, pública o privada, al menos durante cinco años, y necesitarán obtener la pertinente tarjeta de identidad profesional, para lo cual habrán de acreditar, a través de las correspondientes pruebas, conocimientos suficientes sobre la normativa reguladora de la seguridad privada, la organización de servicios de seguridad y las modalidades de prestación de los mismos, no siéndoles aplicable lo dispuesto en este reglamento sobre formación de personal.

2. La habilitación de los directores de seguridad requerirá que los solicitantes cumplan uno de los siguientes requisitos:

a) Estar en posesión de la titulación de seguridad reconocida a estos efectos por el Ministerio del Interior.

b) Acreditar el desempeño durante cinco años, como mínimo, de puestos de dirección o gestión de seguridad pública o privada, y superar las correspondientes pruebas sobre las materias que determine dicho Ministerio.

Sección 4.ª Pérdida de la habilitación

Artículo 64. *Causas.*

1. El personal de seguridad privada perderá tal condición por alguna de las siguientes causas:

a) A petición propia.

b) Por pérdida de alguno de los requisitos generales o específicos exigidos en este reglamento para el otorgamiento de la habilitación o reconocimiento.

c) Por jubilación.

d) Por ejecución de la sanción de retirada definitiva de la habilitación o reconocimiento.

2. La inactividad del personal de seguridad privada por tiempo superior a dos años exigirá la acreditación de los requisitos a que se refiere el apartado 3 del artículo 10 de la Ley de Seguridad Privada, así como la superación de las pruebas específicas que para este supuesto se determinen por el Ministerio del Interior.

Artículo 65. *Devolución de la tarjeta de identidad.*

1. En los casos a que se refiere el apartado 1 del artículo anterior, el personal de seguridad privada deberá hacer entrega, en el plazo de diez días, de su tarjeta de identidad profesional y, en su caso, de la licencia y la guía de pertenencia del arma, al jefe de seguridad o al jefe de personal de la empresa en la que presten servicios, que, a su vez, las

entregará en las dependencias de la Dirección General de la Policía o de la Guardia Civil, según corresponda.

2. Los jefes de seguridad y los guardas particulares del campo no integrados en empresas de seguridad harán la referida entrega personalmente.

3. Cuando sea un detective privado con despacho propio el que pierda su condición, deberá entregar en el mismo plazo, además, salvo en el supuesto de que la actividad del despacho sea continuada por otro despacho de detective privado, el libro-registro necesario con arreglo a lo dispuesto en el artículo 108 del presente Reglamento, y depositar en la Dirección General de la Policía la documentación concerniente a las investigaciones realizadas. Dicha documentación permanecerá en el nuevo despacho de detective privado o en la Dirección General de la Policía, durante un plazo de cinco años, a disposición de las personas que hubieran encargado la investigación y tuvieran derecho a ella; y, transcurrido dicho plazo, se procederá a la destrucción de la misma.

CAPITULO II

Funciones, deberes y responsabilidades

Sección 1.ª Disposiciones comunes

Artículo 66. *Colaboración con las Fuerzas y Cuerpos de Seguridad.*

1. El personal de seguridad privada tendrá obligación especial de auxiliar a las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones en relación con las personas, los bienes, establecimientos o vehículos de cuya protección, vigilancia o custodia estuvieren encargados (artículo 1.4 de la L.S.P.).

2. En cumplimiento de dicha obligación y de lo dispuesto en la Ley Orgánica de Protección de la Seguridad Ciudadana, deberán comunicar a las Fuerzas y Cuerpos de Seguridad, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo de que tuviesen conocimiento en el ejercicio de sus funciones.

3. El personal de seguridad privada que sobresalga en el cumplimiento de sus funciones y especialmente en la colaboración con las Fuerzas y Cuerpos de Seguridad, podrá ser distinguido con menciones honoríficas cuyas características y procedimiento de concesión serán regulados por el Ministerio de Justicia e Interior.

Artículo 67. *Principios de actuación.*

El personal de seguridad privada se atendrá en sus actuaciones a los principios de integridad y dignidad; protección y trato correcto a las personas, evitando abusos, arbitrariedades y violencias y actuando con congruencia y proporcionalidad en la utilización de sus facultades y de los medios disponibles (artículo 1.3 de la L.S.P.).

Artículo 68. *Identificación.*

1. El personal de seguridad privada habrá de portar su tarjeta de identidad profesional y, en su caso, la licencia de armas y la correspondiente guía de pertenencia siempre que se encuentre en el ejercicio de sus funciones, debiendo mostrarlas a los miembros del Cuerpo Nacional de Policía, de la Guardia Civil, y de la Policía de la correspondiente Comunidad Autónoma o Corporación Local, cuando fueren requeridos para ello.

2. Asimismo deberá identificarse con su tarjeta de identidad profesional cuando, por razones del servicio, así lo soliciten los ciudadanos afectados, sin que se puedan utilizar a tal efecto otras tarjetas o placas.

Artículo 69. *Custodia de las armas y de sus documentaciones.*

Durante la prestación del servicio, el personal de seguridad será responsable de la custodia de sus acreditaciones, de las armas que integren su dotación, y de las documentaciones de éstas con objeto de evitar el deterioro, extravío, robo o sustracción de las mismas. Cuando tales hechos se produjeran, deberán dar conocimiento de ellos al jefe de seguridad y a las unidades orgánicas competentes de las Fuerzas y Cuerpos de Seguridad, a efectos de instrucción de los correspondientes expedientes.

Artículo 70. *Incompatibilidades.*

1. Los vigilantes, dentro de la entidad o empresa donde presten sus servicios, se dedicarán exclusivamente a la función de seguridad propia de su cargo, no pudiendo simultanear la misma con otras misiones (artículo 12.2 de la L.S.P.).

No se considerará excluida de la función de seguridad, propia de los vigilantes, la realización de actividades complementarias, directamente relacionadas con aquélla e imprescindibles para su efectividad.

2. Las funciones de escolta privado, vigilante de explosivos y detective privado son incompatibles entre sí y con las demás funciones de personal de seguridad privada aun en los supuestos de habilitación múltiple. Tampoco podrá compatibilizar sus funciones el personal de seguridad privada, salvo los jefes de seguridad, con el ejercicio de cualquier otra actividad dentro de la empresa en que realicen sus servicios.

Sección 2.ª Vigilantes de seguridad

Artículo 71. *Funciones y ejercicio de las mismas.*

1. Los vigilantes de seguridad sólo podrán desempeñar las siguientes funciones:

a) Ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que puedan encontrarse en los mismos.

b) Efectuar controles de identidad en el acceso o en el interior de inmuebles determinados, sin que en ningún caso puedan retener la documentación personal.

c) Evitar la comisión de actos delictivos o infracciones en relación con el objeto de su protección. d) Poner inmediatamente a disposición de los miembros de las Fuerzas y Cuerpos de Seguridad a los delincuentes en relación con el objeto de su protección, así como los instrumentos, efectos y pruebas de los delitos, no pudiendo proceder al interrogatorio de aquéllos.

e) Efectuar la protección del almacenamiento, recuento, clasificación y transporte de dinero, valores y objetos valiosos.

f) Llevar a cabo, en relación con el funcionamiento de centrales de alarma, la prestación de servicios de respuesta de las alarmas que se produzcan, cuya realización no corresponda a las Fuerzas y Cuerpos de Seguridad (artículo 11.1 de la L.S.P.).

2. Deberán seguir las instrucciones que, en el ejercicio de sus competencias impartan los responsables de las Fuerzas y Cuerpos de Seguridad, siempre que se refieran a las personas y bienes de cuya protección y vigilancia estuviesen encargados los vigilantes; colaborando con aquéllas en casos de suspensión de espectáculos, desalojo o cierre provisional de locales y, en general, dentro de los locales o establecimientos en que presten su servicio, en cualquier situación en que sea preciso para el mantenimiento y restablecimiento de la seguridad ciudadana.

3. En la organización de los servicios y en el desempeño de sus funciones, los vigilantes dependerán del jefe de seguridad de la empresa de seguridad en la que estuviesen encuadrados. No obstante, dependerán funcionalmente, en su caso, del jefe del departamento de seguridad de la empresa o entidad en que presten sus servicios.

4. En ausencia del jefe de seguridad, cuando concurran dos o más vigilantes y no estuviese previsto un orden de prelación entre ellos, asumirá la iniciativa en la prestación de los servicios el vigilante más antiguo en el establecimiento o inmueble en el que se desempeñen las funciones.

Artículo 72. *Comprobaciones previas.*

Al hacerse cargo del servicio, y si no existiese responsable de seguridad de la entidad o establecimiento, los vigilantes comprobarán el estado de funcionamiento de los sistemas de seguridad y de comunicación, si los hubiere. Deberán transmitir a los responsables de la entidad o establecimiento y a los de la empresa de seguridad las anomalías observadas, que se anotarán en el librocatálogo de medidas de seguridad. Asimismo advertirán de cualquier otra circunstancia del establecimiento o inmueble que pudiera generar inseguridad.

Artículo 73. *Diligencia.*

Los vigilantes habrán de actuar con la iniciativa y resolución que las circunstancias requieran, evitando la inhibición o pasividad en el servicio y no pudiendo negarse, sin causa que lo justifique, a prestar aquellos que se ajusten a las funciones propias del cargo, de acuerdo con las disposiciones reguladoras de la seguridad privada.

Artículo 74. *Sustituciones.*

1. Los vigilantes deberán comunicar a la empresa en la que estén encuadrados, con la máxima antelación posible, la imposibilidad de acudir al servicio y sus causas, a fin de que aquélla pueda adoptar las medidas pertinentes para su sustitución.
2. Cuando, por enfermedad u otra causa justificada, un vigilante que se encontrara prestando servicio hubiese de ser relevado por otro, lo comunicará a los responsables de seguridad del establecimiento o inmueble y a los de la empresa en que se encuentre encuadrado, con objeto de que puedan asegurar la continuidad del servicio.

Artículo 75. *Equipos caninos.*

1. Para el cumplimiento de sus funciones, los vigilantes de seguridad podrán contar con el apoyo de perros, adecuadamente amaestrados e identificados y debidamente controlados, que habrán de cumplir la regulación sanitaria correspondiente. A tal efecto, los vigilantes de seguridad deberán ser expertos en el tratamiento y utilización de los perros y portar la documentación de éstos.
2. En tales casos se habrán de constituir equipos caninos, de forma que se eviten los riesgos que los perros puedan suponer para las personas, al tiempo que se garantiza su eficacia para el servicio.

Artículo 76. *Prevenciones y actuaciones en casos de delito.*

1. En el ejercicio de su función de protección de bienes inmuebles así como de las personas que se encuentren en ellos, los vigilantes de seguridad deberán realizar las comprobaciones, registros y prevenciones necesarias para el cumplimiento de su misión.
2. No obstante, cuando observaren la comisión de delitos en relación con la seguridad de las personas o bienes objeto de protección, o cuando concurran indicios racionales de tal comisión, deberán poner inmediatamente a disposición de los miembros de las Fuerzas y Cuerpos de Seguridad a los presuntos delincuentes, así como los instrumentos, efectos y pruebas de los supuestos delitos.

Artículo 77. *Controles en el acceso a inmuebles.*

En los controles de accesos o en el interior de los inmuebles de cuya vigilancia y seguridad estuvieran encargados, los vigilantes de seguridad podrán realizar controles de identidad de las personas y, si procede, impedir su entrada, sin retener la documentación personal y, en su caso, tomarán nota del nombre, apellidos y número del documento nacional de identidad o documento equivalente de la persona identificada, objeto de la visita y lugar del inmueble a que se dirigen, dotándola, cuando así se determine en las instrucciones de seguridad propias del inmueble, de una credencial que le permita el acceso y circulación interior, debiendo retirarla al finalizar la visita.

Artículo 78. *Represión del tráfico de estupefacientes.*

Los vigilantes de seguridad deberán impedir el consumo ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas en el interior de los locales o establecimientos o instalaciones objeto de su vigilancia y protección.

Artículo 79. *Actuación en el exterior de inmuebles.*

1. Los vigilantes sólo podrán desempeñar sus funciones en el interior de los edificios o de los inmuebles de cuya vigilancia y seguridad estuvieran encargados, salvo en los siguientes casos:

a) El transporte y distribución de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen o por su peligrosidad, puedan requerir protección especial.

b) La manipulación o utilización de bienes, maquinaria o equipos valiosos que hayan de tener lugar en las vías públicas o de uso común, cuando tales operaciones, bienes o equipos hayan de ser protegidos por vigilantes de seguridad, desde el espacio exterior, inmediatamente circundante.

c) Los servicios de verificación de alarmas y de respuesta a las mismas a que se refiere el artículo 49 de este Reglamento.

d) Los supuestos de persecución a delincuentes sorprendidos en flagrante delito, como consecuencia del cumplimiento de sus funciones en relación con las personas o bienes objeto de su vigilancia y protección.

e) Las situaciones en que ello viniera exigido por razones humanitarias relacionadas con dichas personas o bienes.

f) La retirada y reposición de fondos en cajeros automáticos, así como la prestación de servicios de vigilancia y protección de los cajeros durante las citadas operaciones, o en las de reparación de averías, fuera de las horas habituales de horario al público en las respectivas oficinas.

g) Los desplazamientos excepcionales al exterior de los inmuebles objeto de protección para la realización de actividades directamente relacionadas con las funciones de vigilancia y seguridad, teniendo en cuenta, en su caso, las instrucciones de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

2. Las limitaciones previstas en el apartado precedente no serán aplicables a los servicios de vigilancia y protección de seguridad privada de los medios de transporte y de sus infraestructuras que tengan vías específicas y exclusivas de circulación, coordinados cuando proceda con los servicios de las Fuerzas y Cuerpos de Seguridad.

Artículo 80. *Servicio en polígonos industriales o urbanizaciones.*

1. El servicio de seguridad en vías de uso común pertenecientes a polígonos industriales o urbanizaciones aisladas será prestado por una sola empresa de seguridad y habrá de realizarse, durante el horario nocturno, por medio de dos vigilantes, al menos, debiendo estar conectados entre sí y con la empresa de seguridad por radiocomunicación y disponer de medios de desplazamiento adecuados a la extensión del polígono o urbanización.

2. La prestación del servicio en los polígonos industriales o urbanizaciones habrá de estar autorizada por el Gobernador civil de la provincia, previa comprobación, mediante informe de las unidades competentes de las Fuerzas y Cuerpos de Seguridad, de que concurren los siguientes requisitos:

a) Que los polígonos o urbanizaciones estén netamente delimitados y separados de los núcleos poblados.

b) Que no se produzca solución de continuidad, entre distintas partes del polígono o urbanización, por vías de comunicación ajenas a los mismos, o por otros factores. En caso de que exista o se produzca solución de continuidad, cada parte deberá ser considerada un polígono o urbanización autónomo a efectos de aplicación del presente artículo.

c) Que no se efectúe un uso público de las calles del polígono o urbanización por tráfico o circulación frecuente de vehículos ajenos a los mismos.

d) Que la administración municipal no se haya hecho cargo de la gestión de los elementos comunes y de la prestación de los servicios municipales.

e) Que el polígono o urbanización cuente con administración específica y global que permita la adopción de decisiones comunes.

3. Con independencia de lo dispuesto en el apartado 1, los titulares de los bienes que integren el polígono o urbanización podrán concertar con distintas empresas de seguridad la protección de sus respectivos locales, edificios o instalaciones, pero en este caso los vigilantes de seguridad desempeñarán sus funciones en el interior de los indicados locales, edificios o instalaciones.

4. Cuando en el cumplimiento de su misión en polígonos industriales o urbanizaciones, y con independencia del ejercicio de la función que les corresponda en el control de accesos, fuese precisa la identificación de alguna persona, los vigilantes la reflejarán en un parte de servicio, que se entregará seguidamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 81. *Prestación de servicios con armas.*

1. Los vigilantes sólo desempeñarán con armas de fuego los siguientes servicios:

a) Los de protección del almacenamiento, recuento, clasificación, transporte y distribución de dinero, valores y objetos valiosos o peligrosos.

b) Los de vigilancia y protección de:

1.º Centros y establecimientos militares y aquellos otros dependientes del Ministerio de Defensa, en los que presten servicio miembros de las Fuerzas Armadas o estén destinados al uso por el citado personal.

2.º Fábricas, depósitos y transporte de armas, explosivos y sustancias peligrosas.

3.º Industrias o establecimientos calificados como peligrosos, con arreglo a la legislación de actividades clasificadas, por manipulación, utilización o producción de materias inflamables o explosivas que se encuentren en despoblado.

c) En los siguientes establecimientos, entidades, organismos, inmuebles y buques, cuando así se disponga por la Dirección General de la Policía y de la Guardia Civil en los supuestos no circunscritos al ámbito provincial, o por las Delegaciones o Subdelegaciones del Gobierno, valoradas circunstancias tales como la localización, el valor de los objetos a proteger, la concentración del riesgo o peligrosidad, la nocturnidad u otras de análoga significación:

1.º Dependencias de Bancos, Cajas de Ahorro y entidades de crédito.

2.º Centros de producción, transformación y distribución de energía.

3.º Centros y sedes de repetidores de comunicación.

4.º Polígonos industriales y lugares donde se concentre almacenamiento de materias primas o mercancías.

5.º Urbanizaciones aisladas.

6.º Joyerías, platerías o lugares donde se fabriquen, almacenen o exhiban objetos preciosos.

7.º Museos, salas de exposiciones o similares.

8.º Los lugares de caja o donde se concentren fondos, de grandes superficies comerciales o de casinos de juego.

9.º Buques mercantes y buques pesqueros que naveguen bajo bandera española en aguas en las que exista grave riesgo para la seguridad de las personas o de los bienes, o para ambos.

2. Cuando las empresas, organismos o entidades titulares de los establecimientos o inmuebles entendiesen que en supuestos no incluidos en el apartado anterior el servicio debiera ser prestado con armas de fuego, teniendo en cuenta las circunstancias que en el mismo se mencionan, solicitarán la correspondiente autorización a la Dirección General de la Policía y de la Guardia Civil, respecto a supuestos no circunscritos al ámbito provincial o a las Delegaciones o Subdelegaciones del Gobierno, que resolverán lo procedente, pudiendo autorizar la formalización del correspondiente contrato.

Artículo 82. *Depósito de las armas.*

1. Los vigilantes no podrán portar las armas fuera de las horas y de los lugares de prestación del servicio, debiendo el tiempo restante estar depositadas en los armeros de los lugares de trabajo o, si no existieran, en los de la empresa de seguridad.

2. Excepcionalmente, a la iniciación y terminación del contrato de servicio o, cuando se trate de realizar servicios especiales, suplencias, o los ejercicios obligatorios de tiro, podrán portar las armas en los desplazamientos anteriores y posteriores, previa autorización del jefe de seguridad o, en su defecto, del responsable de la empresa de seguridad, que habrá de ajustarse a las formalidades que determine el Ministerio de Justicia e Interior, debiendo entregarlas para su depósito en el correspondiente armero.

A los efectos previstos en el párrafo anterior, se considerarán servicios especiales aquéllos cuya duración no exceda de un mes.

Artículo 83. *Responsabilidad por la custodia de las armas.*

1. Las empresas de seguridad serán responsables de la conservación, mantenimiento y buen funcionamiento de las armas, y los vigilantes, de la seguridad, cuidado y uso correcto de las que tuvieran asignadas, durante la prestación del servicio.

2. De la obligación de depositar el arma en el armero del lugar de trabajo serán responsables el vigilante y el jefe de seguridad, y de la relativa a depósito en el armero de la empresa de seguridad, el vigilante y el jefe de seguridad o director de la empresa de seguridad.

3. Del extravío, robo o sustracción de las armas, así como, en todo caso, de su ausencia del armero cuando deban estar depositadas en el mismo se deberá dar cuenta inmediata a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 84. *Ejercicios de tiro.*

1. Los vigilantes de seguridad que presten servicios con armas deberán realizar un ejercicio de tiro obligatorio al semestre, y los demás que puedan prestar dichos servicios, por estar en posesión de las correspondientes licencias de armas, aunque las mismas se encuentren depositadas en las Intervenciones de Armas de la Guardia Civil, un ejercicio de tiro obligatorio al año. En ambos casos, se efectuará el número de disparos que se determine por el Ministerio del Interior. No deberán transcurrir más de ocho meses entre dos ejercicios sucesivos de los primeros, ni más de catorce meses entre dos ejercicios sucesivos de los segundos.

La falta de realización o el resultado negativo de un ejercicio de tiro podrá dar lugar a la suspensión temporal de la correspondiente licencia de armas hasta que el ejercicio se realice con resultado positivo.

2. Si fuere necesario, para los ejercicios obligatorios de tiro de los vigilantes que no tuviesen asignadas armas, se trasladarán por el jefe o responsable de seguridad de la empresa las que ésta posea con tal objeto, efectuándose el traslado con la protección de un vigilante armado, yendo las armas descargadas y separadas de la cartuchería, de acuerdo con lo dispuesto en el Reglamento de Armas.

Artículo 85. *Pruebas psicotécnicas periódicas.*

Los vigilantes que presten o puedan prestar servicio con armas deberán superar, con una periodicidad de cinco años, las pruebas psicotécnicas que determine el Ministerio de Justicia e Interior, periodicidad que será bienal a partir de los cincuenta y cinco años de edad, cuyo resultado se comunicará a la Intervención de Armas. En caso de no realización o superación de las pruebas, los interesados no podrán desempeñar servicios con armas, debiendo hacer entrega de la correspondiente licencia, para su anulación, a la Intervención de Armas.

Artículo 86. *Arma de fuego y medios de defensa.*

1. El arma reglamentaria de los vigilantes de seguridad en los servicios que hayan de prestarse con armas será la que determine el Ministerio del Interior.

2. Los vigilantes de seguridad portarán la defensa que se determine por el Ministerio del Interior, en los supuestos que asimismo se determinen por dicho Ministerio.

3. Cuando los vigilantes en el ejercicio de sus funciones hayan de proceder a la detención e inmovilización de personas para su puesta a disposición de las Fuerzas y Cuerpos de Seguridad, el jefe de seguridad podrá disponer el uso de grilletes.

4. En los supuestos previstos en el nº 9 de la letra c) del apartado 1 del artículo 81 anterior, los vigilantes de seguridad privada podrán portar y usar armas de guerra para la prestación de servicios de protección de personas y bienes, previniendo y repeliendo ataques, con las características, en las condiciones y con los requisitos que se determinen, de manera conjunta, por los Ministerios de Defensa y de Interior.

Artículo 87. *Uniforme y distintivos.*

1. Las funciones de los vigilantes de seguridad únicamente podrán ser desarrolladas vistiendo el uniforme y ostentando el distintivo del cargo que sean preceptivos, que serán aprobados por el Ministerio de Justicia e Interior, teniendo en cuenta las características de las funciones respectivas de las distintas especialidades de vigilantes y que no podrán confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad (artículo 12.1 de la L.S.P.).

2. Los vigilantes no podrán vestir el uniforme ni hacer uso de sus distintivos fuera de las horas y lugares del servicio y de los ejercicios de tiro.

Sección 3.ª Escoltas privados

Artículo 88. *Funciones.*

1. Son funciones de los escoltas privados, con carácter exclusivo y excluyente, el acompañamiento, defensa y protección de personas determinadas, que no tengan la condición de autoridades públicas, impidiendo que sean objeto de agresiones o actos delictivos (artículo 17.1 de la L.S.P.).

2. La defensa y protección a prestar ha de estar referida únicamente a la vida e integridad física y a la libertad de las personas objeto de protección.

Artículo 89. *Forma de prestación del servicio.*

En el desempeño de sus funciones, los escoltas no podrán realizar identificaciones o detenciones, ni impedir o restringir la libre circulación, salvo que resultase imprescindible como consecuencia de una agresión o de un intento manifiesto de agresión a la persona protegida o a los propios escoltas, debiendo en tal caso poner inmediatamente al detenido o detenidos a disposición de las Fuerzas y Cuerpos de Seguridad, sin proceder a ninguna suerte de interrogatorio.

Artículo 90. *Uso de armas y ejercicios de tiro.*

1. El arma reglamentaria de los escoltas privados será la que determine el Ministerio de Justicia e Interior.

2. Portarán las armas con discreción y sin hacer ostentación de ellas, pudiendo usarlas solamente en caso de agresión a la vida, integridad física o libertad, y atendiendo a criterios de proporcionalidad con el medio utilizado para el ataque.

3. Los escoltas privados podrán portar sus armas solamente cuando se encuentren en el ejercicio de sus funciones, debiendo depositarlas, a la finalización de cada servicio, en el armero de la empresa a la que pertenezcan, o en el del lugar de trabajo o residencia de la persona protegida.

4. Cuando por razones de trabajo se hallasen, al finalizar el servicio, en localidad distinta de aquélla en la que radique la sede de su empresa, el arma se depositará en el armero de

la delegación de la empresa, si la hubiese. En caso contrario, el arma quedará bajo la custodia del escolta, con la autorización, con arreglo al artículo 82, del jefe de seguridad de la empresa.

5. Los escoltas privados deberán realizar ejercicios obligatorios de tiro, una vez cada trimestre, y les será de aplicación lo dispuesto en este Reglamento para los vigilantes de seguridad, sobre número de disparos, conservación y mantenimiento de las armas que tuvieren asignadas, así como lo establecido respecto a la autorización para su traslado con ocasión de los ejercicios obligatorios de tiro.

Artículo 91. *Régimen general.*

A los escoltas privados les será de aplicación lo establecido para los vigilantes de seguridad sobre:

a) Colaboración con las Fuerzas y Cuerpos de Seguridad.
b) Diligencia en la prestación del servicio.
c) Sustituciones.
d) Conservación de las armas.
e) Pruebas psicotécnicas periódicas.

Sección 4.ª Guardas particulares del campo

Artículo 92. *Funciones.*

Los guardas particulares del campo, en sus distintas modalidades, ejercerán las funciones de vigilancia y protección de la propiedad:

a) En las fincas rústicas.
b) En las fincas de caza, en cuanto a los distintos aspectos del régimen cinegético.
c) En los establecimientos de acuicultura y zonas marítimas protegidas con fines pesqueros.

Artículo 93. *Arma reglamentaria.*

1. El arma reglamentaria de los guardas particulares del campo será el arma de fuego larga para vigilancia y guardería, determinada con arreglo a lo dispuesto en el artículo 3 del Reglamento de Armas.

2. Cuando el guarda esté encuadrado en una empresa de seguridad, al finalizar el servicio depositará el arma en el armero de aquélla, si tuviese su sede o delegación en la localidad de prestación del servicio; y, en caso contrario, el arma quedará bajo la custodia del guarda.

3. Solamente se podrán prestar con armas los servicios de vigilancia de terrenos cinegéticos y aquellos otros que autorice el Gobernador Civil, teniendo en cuenta los supuestos y circunstancias enumerados en el artículo 81 de este Reglamento.

Artículo 94. *Régimen general.*

A los guardas particulares del campo les será de aplicación lo establecido para los vigilantes de seguridad sobre:

a) Colaboración con las Fuerzas y Cuerpos de Seguridad.
b) Disposición de cartilla de tiro.
c) Diligencia en la prestación del servicio.
d) Sustituciones.
e) Utilización de perros.
f) Controles y actuaciones en casos de delito.
g) Ejercicios de tiro, cuya periodicidad será anual.
h) Conservación de armas.
i) Pruebas psicotécnicas periódicas.
j) Utilización de uniformes y distintivos.
k) Comprobaciones previas a la iniciación de los servicios.

Sección 5.ª Jefes y directores de seguridad

Artículo 95. *Funciones.*

1. A los jefes de seguridad les corresponde, bajo la dirección de las empresas de que dependan, el ejercicio de las siguientes funciones:

a) El análisis de situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implantación y realización de los servicios de seguridad.
b) La organización, dirección e inspección del personal y servicios de seguridad privada.
c) La propuesta de los sistemas de seguridad que resulten pertinentes, así como la supervisión de su utilización, funcionamiento y conservación.
d) El control de la formación permanente del personal de seguridad que de ellos dependa, proponiendo a la dirección de la empresa la adopción de las medidas o iniciativas adecuadas para el cumplimiento de dicha finalidad.
e) La coordinación de los distintos servicios de seguridad que de ellos dependan, con actuaciones propias de protección civil, en situaciones de emergencia, catástrofe o calamidad pública.
f) Asegurar la colaboración de los servicios de seguridad con los de las correspondientes dependencias de las Fuerzas y Cuerpos de Seguridad.
g) En general, velar por la observancia de la regulación de seguridad aplicable.
h) La dirección de los ejercicios de tiro del personal de seguridad a sus órdenes, si poseyeran la cualificación necesaria como instructores de tiro.

2. A los directores de seguridad les corresponde el ejercicio de las funciones enumeradas en los apartados a), b), c), e), f) y g) del artículo anterior.

Artículo 96. *Supuestos de existencia obligatoria.*

1. Los servicios de seguridad se prestarán obligatoriamente bajo la dirección de un jefe de seguridad, en las empresas de seguridad inscritas para todas o alguna de las actividades previstas en el artículo 1.1, párrafos a), b), c) y d), del presente reglamento, y en las delegaciones o sucursales abiertas de acuerdo con lo dispuesto en el artículo 17, apartados 2 y 3 de este reglamento.
2. El mando de los servicios de seguridad se ejercerá por un director de seguridad designado por la entidad, empresa o grupo empresarial:

a) En las empresas o entidades que constituyan, en virtud de disposición general o decisión gubernativa, departamento de seguridad.
b) En los centros, establecimientos o inmuebles que cuenten con un servicio de seguridad integrado por veinticuatro o más vigilantes de seguridad o guardas particulares del campo, y cuya duración prevista supere un año. c) Cuando así lo disponga la Dirección General de la Policía y de la Guardia Civil para los supuestos supraprovinciales, o el Subdelegado del Gobierno de la provincia, atendiendo el volumen de medios personales y materiales, tanto físicos como electrónicos, el sistema de seguridad de la entidad o establecimiento, así como la complejidad de su funcionamiento y el grado de concentración de riesgo.

Artículo 97. *Comunicación con las Fuerzas y Cuerpos de Seguridad.*

Los jefes de seguridad, así como los directores de seguridad, canalizarán hacia las dependencias de las Fuerzas y Cuerpos de Seguridad las comunicaciones a que se refiere el artículo 66 de este Reglamento, y deberán comparecer a las reuniones informativas o de coordinación a que fueren citados por las autoridades policiales competentes.

Artículo 98. *Subsanación de deficiencias o anomalías.*

Los jefes y los directores de seguridad deberán proponer o adoptar las medidas oportunas para la subsanación de las deficiencias o anomalías que observen o les comuniquen los vigilantes o los guardas particulares del campo en relación con los servicios

o los sistemas de seguridad, asegurándose de la anotación, en este último caso, de la fecha y hora de la subsanación en el correspondiente libro-catálogo y comprobando su funcionamiento.

Artículo 99. *Delegación de funciones.*

Los jefes de seguridad podrán delegar únicamente el ejercicio de las facultades para autorizar el traslado de armas o la obligación de efectuar personalmente el traslado, y las relativas a comunicación con las Fuerzas y Cuerpos de Seguridad y a subsanación de deficiencias o anomalías, así como las de dirección e inspección del personal y servicios de seguridad privada, lo que requerirá la aprobación de las empresas, y habrá de recaer, donde no hubiera jefe de seguridad delegado, en persona del Servicio o Departamento de Seguridad que reúna análogas condiciones de experiencia y capacidad que ellos; comunicando a las dependencias de las Fuerzas y Cuerpos de Seguridad el alcance de la delegación y la persona o personas de la empresa en quienes recae, con expresión del puesto que ocupa en la propia empresa. Asimismo deberán comunicar a dichas dependencias cualquier variación que se produzca al respecto, y en su caso la revocación de la delegación.

Artículo 100. *Comunicación de altas y bajas.*

Las empresas de seguridad y las entidades con departamento de seguridad comunicarán a la Dirección General de la Policía las altas y bajas de los jefes de seguridad y de los directores de seguridad, respectivamente, dentro de los cinco días siguientes a la fecha en que se produzcan.

Sección 6.ª Detectives privados

Artículo 101. *Funciones.*

1. Los detectives privados, a solicitud de personas físicas o jurídicas, se encargarán:

a) De obtener y aportar información y pruebas sobre conductas o hechos privados.
b) De la investigación de delitos perseguibles sólo a instancia de parte por encargo de los legitimados en el proceso penal.
c) De la vigilancia en ferias, hoteles, exposiciones o ámbitos análogos (artículo 19.1 de la L.S.P.).

2. A los efectos del presente artículo, se considerarán conductas o hechos privados los que afecten al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.
3. En el ámbito del apartado 1.c) se consideran comprendidas las grandes superficies comerciales y los locales públicos de gran concurrencia.

Artículo 102. *Prohibiciones.*

1. Los detectives no podrán realizar investigaciones sobre delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido, relacionados con dichos delitos.
2. En ningún caso podrán utilizar para sus investigaciones medios personales o técnicos que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones (artículo 19.3 y 4 de la Ley de S.P.).

Artículo 103. *Carácter reservado de las investigaciones.*

Los detectives privados están obligados a guardar riguroso secreto de las investigaciones que realicen y no podrán facilitar datos sobre éstas más que a las personas que se las encomienden y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

Artículo 104. *Registro especial.*

1. Por la Dirección General de la Policía se llevará un Registro de detectives privados con despacho abierto, en el que, con el número de orden de inscripción, figurará su nombre y apellidos, domicilio social y, en su caso, detectives asociados o dependientes, habilitados de acuerdo con lo dispuesto en los preceptos aplicables de los artículos 52 a 65 de este Reglamento, y delegaciones o sucursales que de aquéllos dependan, así como el nombre comercial que utilicen. La Dirección General de la Policía comunicará oportunamente estos datos al órgano correspondiente de la Comunidad Autónoma competente.

2. Para el comienzo del desarrollo de las funciones del detective privado y de sus detectives asociados, la apertura del despacho deberá estar reseñada en el Registro a que se refiere el apartado anterior, y hallarse en posesión el titular y los asociados de las correspondientes tarjetas de identidad profesional. No se podrá hacer publicidad de las actividades propias de los detectives privados sin estar inscrito en el Registro.

3. La inscripción del despacho en dicho Registro se practicará previa instrucción de procedimiento, iniciado a solicitud de persona interesada, en el que habrá de acreditarse, si ya no lo estuviere en el órgano encargado del Registro, el cumplimiento de los requisitos generales que se determinan en el artículo 53 de este Reglamento, y de los específicos señalados en el artículo 54.5 del mismo, así como el de haber causado alta en el Impuesto de Actividades Económicas.

4. La inscripción de detectives dependientes o asociados se acordará previa solicitud del detective titular del despacho de que dependan, adjuntando, en caso de vinculación laboral, documento acreditativo del alta de aquéllos en la Seguridad Social.

5. A los procedimientos de inscripción de despachos de detectives privados les será de aplicación lo dispuesto en los artículos 8 y 9 de este Reglamento, sobre subsanación de defectos, resoluciones, notificaciones y recursos.

6. El número de orden de inscripción y la fecha en que se hubiere acordado se comunicará al interesado, que deberá hacer constar dicho número en su publicidad, documentos e informes.

7. Cualquier variación de los datos registrales, así como de los relativos a detectives dependientes o asociados y a delegaciones o sucursales, se comunicará, en el plazo de los quince días siguientes a la fecha en que se produzca, a efectos de su posible incorporación al Registro especial, a la Dirección General de la Policía, que la transmitirá oportunamente al órgano correspondiente de la Comunidad Autónoma competente.

Artículo 105. *Sociedades de detectives.*

1. Las sociedades mercantiles, laborales o cooperativas de detectives habrán de estar constituidas únicamente por personas físicas reglamentariamente habilitadas como tales, debiendo remitir a la Dirección General de la Policía, a efectos de inscripción en el Registro, copia autorizada de la escritura de constitución de la sociedad y certificado o nota de inscripción de la misma en el Registro correspondiente, así como de cualquier modificación que se produzca en la composición de los órganos de administración de la sociedad o en la titularidad de las acciones o participaciones representativas de su capital y en los aumentos o disminuciones de éste. La comunicación deberá remitirse a la Dirección General de la Policía en los quince días siguientes a la fecha en que se otorgue la correspondiente escritura o se produzca la modificación en cuestión, correspondiendo al citado centro directivo dar traslado de la comunicación a la Comunidad Autónoma competente.

2. Los miembros de estas sociedades únicamente podrán dedicarse a la realización de las actividades propias de los detectives, no pudiendo desarrollar ninguna de las atribuidas con carácter exclusivo a las empresas de seguridad.

Artículo 106. *Establecimiento de sucursales.*

Los detectives privados podrán establecer departamentos delegados o sucursales en la misma localidad donde tengan establecido su despacho profesional o en otras distintas, debiendo, en todo caso, estar dirigido cada uno de ellos por un detective habilitado o

reconocido con arreglo a lo dispuesto en este reglamento, distinto del titular de la oficina principal.

Artículo 107. *Apertura de sucursales.*

Para la efectividad de lo dispuesto en el artículo anterior, deberán comunicar previamente a la Dirección General de la Policía, que dará traslado a la Comunidad Autónoma competente, la apertura de la delegación o sucursal, con la determinación de su localización, y acompañando los documentos relativos a los detectives que vayan a trabajar en la misma.

Artículo 108. *Libro-registro.*

1. En cada despacho y sucursal, los detectives llevarán un libro-registro, según el modelo que se apruebe por el Ministerio del Interior, concebido de forma que su tratamiento y archivo pueda ser mecanizado e informatizado.

2. La obligación de llevanza del libro-registro del apartado anterior también corresponderá a los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo habilitados como detectives privados en cualquiera de dichos Estados y que pretendan ejercer su profesión en España sin disponer de despacho o sucursal en nuestro país.

Artículo 109. *Comunicación de informaciones.*

Los detectives titulares y los asociados o dependientes, cuando sean requeridos para ello por los órganos competentes de la Administración de Justicia, y de las Fuerzas y Cuerpos de Seguridad, deberán facilitar las informaciones de que tuvieran conocimiento en relación con las investigaciones que tales organismos se encontraran llevando a cabo.

Artículo 110. *Responsabilidad.*

Los detectives privados y las sociedades de detectives responderán civilmente de las acciones u omisiones en que, durante la ejecución de sus servicios, incurran los detectives dependientes o asociados que con ellos estén vinculados.

TITULO III

Medidas de seguridad

CAPITULO I

Medidas de seguridad en general

Sección 1.ª Disposiciones comunes

Artículo 111. *Obligatoriedad.*

1. De acuerdo con lo dispuesto en el artículo 13 y en la disposición adicional de la Ley Orgánica 1/1992, sobre protección de la seguridad ciudadana, y con la finalidad de prevenir la comisión de actos delictivos, la Secretaría de Estado de Interior, para supuestos supraprovinciales, o los Gobernadores Civiles podrán ordenar que las empresas industriales, comerciales o de servicios adopten las medidas de seguridad que, con carácter general o para supuestos específicos, se establecen en el presente Reglamento.

2. Las obras que resulte preciso efectuar en los establecimientos, para la adopción de las medidas de seguridad obligatorias, serán comunicadas al arrendador, si bien éste no podrá oponerse a ellas, salvo que provoquen una disminución de la estabilidad o seguridad del edificio. Al concluir el contrato, el arrendador podrá optar entre exigir al arrendatario que

reponga las cosas al estado anterior, o conservar la modificación efectuada, sin que éste pueda reclamar indemnización alguna.

Sección 2.ª Servicios y sistemas de seguridad

Artículo 112. *Enumeración de los servicios o sistemas y circunstancias determinantes.*

1. Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:

a) Creación del departamento de seguridad.
b) Establecimiento del servicio de vigilantes de seguridad, con o sin armas a cargo de personal integrado en empresas de seguridad.
c) Instalación de dispositivos y sistemas de seguridad y protección.
d) Conexión de los sistemas de seguridad con centrales de alarmas, ajenas o propias, que deberán ajustarse en su funcionamiento a los establecido en los artículos 46, 48 y 49, y reunir los requisitos que se establecen en el apartado 6.2 del anexo del presente Reglamento; no pudiendo prestar servicios a terceros si las empresas o entidades no están habilitadas como empresas de seguridad.

2. En todo caso deberá existir Departamento de Seguridad cuando concurran las circunstancias de los párrafos b) y c) del artículo 96.2 de este Reglamento.

Artículo 113. *Implantación en organismos públicos.*

Si se considerase necesaria la implantación de dichos servicios o sistemas de seguridad en empresas, entidades u organismos públicos, el Director general de la Policía para supuestos supraprovinciales, o los Gobernadores Civiles elevarán al Ministro de Justicia e Interior la correspondiente propuesta para que, previo acuerdo con el Ministerio o Administración de los que dependan las instalaciones o locales necesitados de protección, dicte la resolución procedente.

En forma análoga se procederá por los órganos correspondientes de las Comunidades Autónomas competentes, cuando se trate de empresas, entidades u organismos públicos dependientes de la Administración Autonómica o de la Administración Local.

Artículo 114. *Servicio sustitutorio de vigilantes de seguridad.*

Cuando por dificultades técnicas o carencia de equipos adecuados fuera imposible la conexión del sistema de seguridad con una central privada de alarmas, las empresas y entidades a que se refiere el artículo 112, que debieran establecer tal sistema de seguridad, podrán ser obligadas, por el tiempo en que persista la imposibilidad técnica, a la implantación del servicio de vigilantes de seguridad, con personal perteneciente a empresas de seguridad.

Artículo 115. *Departamento de seguridad facultativo.*

Las empresas industriales, comerciales o de servicios, y las entidades públicas y privadas, que, sin estar obligadas a ello -por no estar comprendidas en los supuestos regulados en el artículo 96 del presente Reglamento-, pretendan organizar su departamento de seguridad, con todos o alguno de los cometidos enumerados en el artículo siguiente, deberán disponer de un director de seguridad al frente del mismo, y comunicarlo a la Subdelegación del Gobierno, si el ámbito de actuación no excediera del territorio de una provincia, y, en todo caso, al Director general de la Policía.

Artículo 116. *Cometidos del departamento de seguridad.*

El departamento de seguridad obligatoriamente establecido, único para cada entidad, empresa o grupo empresarial y con competencia en todo el ámbito geográfico en que éstos actúen, comprenderá la administración y organización de los servicios de seguridad de la empresa o grupo, incluso, en su caso, del transporte y custodia de efectos y valores, correspondiéndole la dirección de los vigilantes de seguridad o guardas particulares del campo, el control del funcionamiento de las instalaciones de sistemas físicos y electrónicos, así como del mantenimiento de éstos y la gestión de las informaciones que generen.

Artículo 117. *Organización del departamento de seguridad.*

En aquellas entidades y empresas de seguridad en las que el departamento de seguridad se caracterice por su gran volumen y complejidad, en dicho departamento existirá, bajo la dirección de seguridad, a la que corresponderán las funciones del director de seguridad, la estructura necesaria con los escalones jerárquicos y territoriales adecuados, al frente de los cuales se encontrarán los delegados correspondientes.

Artículo 118. *Dispensa del servicio de vigilantes de seguridad.*

1. En los casos en que, en uso de las facultades que confiere este Reglamento, se requiera la implantación del servicio de vigilantes de seguridad, el Director general de la Policía en supuestos supraprovinciales, o los Gobernadores Civiles, a petición de la empresa o entidad interesada, dispensarán de la implantación o mantenimiento del servicio de vigilantes de seguridad o de guardas particulares del campo en los centros o establecimientos, cuando aquélla acredite la instalación y el adecuado funcionamiento de las medidas de seguridad específicamente reguladas en el presente Reglamento.

2. La solicitud de dispensa se presentará ante dichas autoridades, que comprobarán la instalación y el adecuado funcionamiento de tales medidas de seguridad a través de la inspección que realicen los funcionarios competentes del Cuerpo Nacional de Policía, o, en su caso, del Cuerpo de la Guardia Civil, y resolverán lo procedente, recabando previamente el parecer de los representantes de los trabajadores, que habrán de expresarlo dentro de un plazo de diez días.

CAPITULO II

Medidas de seguridad específicas

Sección 1.ª Bancos, cajas de ahorro y demás entidades de credito

Artículo 119. *Departamento de seguridad y central de alarmas.*

1. En todos los bancos, cajas de ahorro y demás entidades de crédito, existirá un departamento de seguridad, que tendrá a su cargo la organización y administración de la seguridad de la entidad bancaria o de crédito, de acuerdo con lo dispuesto en el artículo 116 de este Reglamento.

2. Asimismo, dichas entidades deberán conectar con una central de alarmas propia o ajena los sistemas de seguridad instalados en sus establecimientos y oficinas, salvo que dificultades técnicas hicieran imposible la conexión, en cuyo caso les será de aplicación lo dispuesto en el artículo 114.

3. Las centrales de alarmas propias de una entidad de crédito, que habrán de ajustarse en su funcionamiento a lo establecido en los artículos 46, 48 y 49, y reunir los requisitos del apartado 6.2 del anexo de este Reglamento, podrán prestar servicios a los distintos establecimientos de la misma entidad o de sus filiales.

Artículo 120. *Medidas de seguridad concretas.*

1. En los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso

teniendo en cuenta las circunstancias enumeradas en el artículo 112 de este Reglamento y los criterios que se fijen por el Ministerio de Justicia e Interior, oyendo a la Comisión Mixta Central de Seguridad Privada:

a) Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquéllos, y que habrán de funcionar durante el horario de atención al público, sin que requieran la intervención inmediata de los empleados de la entidad.

Los soportes destinados a la grabación de imágenes han de estar protegidos contra robo, y la entidad de ahorro o de crédito deberá conservar los soportes con las imágenes grabadas durante quince días al menos desde la fecha de la grabación, en que estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos.

El contenido de los soportes será estrictamente reservado, y las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, debiendo ser inutilizados el contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.

b) Dispositivos electrónicos, de las características que se determinen por el Ministerio de Justicia e Interior, con capacidad para detectar el ataque a cualquier elemento de seguridad física donde se custodien efectivo o valores.

c) Pulsadores u otros medios de accionamiento fácil de las señales de alarma.

d) Recinto de caja de, al menos, dos metros de altura y que deberá estar cerrado desde su interior durante las horas de atención al público, siempre que el personal se encuentre dentro del mismo, protegido con blindaje antibala del nivel que se determine y dispositivo capaz de impedir el ataque a las personas situadas en su interior.

e) Control individualizado de accesos a la oficina o establecimiento, que permita la detección de masas metálicas, bloqueo y anclaje automático de puertas, y disponga de mando a distancia para el desbloqueo del sistema en caso de incendio o catástrofe, o puerta de emergencia complementaria, detectores de presencia o zócalos sensibles en vía de salida cuando se utilice el sistema de doble vía, y blindaje que se determine.

f) Carteles del tamaño que se determine por el Ministerio de Justicia e Interior u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad, con referencia expresa al sistema de apertura automática retardada y, en su caso, al sistema permanente de captación de imágenes.

2. Los establecimientos y oficinas de crédito situadas en localidades con población inferior a diez mil habitantes, y que además no cuenten con más de diez empleados, estarán exceptuadas de la obligación de implantar las medidas de seguridad enumeradas bajo los párrafos d) y e) del apartado anterior.

En las restantes oficinas o establecimientos, las entidades deberán instalar, en su caso, una de las dos medidas de seguridad incluidas bajo los párrafos d) y e) del apartado 1, pudiendo optar voluntariamente por cualquiera de ellas. No obstante, la Dirección General de la Policía en supuestos que excedan del territorio de una provincia, o el Gobierno Civil, a petición de la entidad interesada, oyendo a la representación de los trabajadores que habrá de expresar su parecer dentro de un plazo de diez días, y previa valoración de las circunstancias a que se refiere el artículo 112.1 de este Reglamento, podrá autorizar la sustitución de cualquiera de dichas medidas por la implantación del servicio de vigilantes de seguridad.

3. En la determinación de las medidas de seguridad a implantar en las oficinas de las entidades de crédito sitas en las Delegaciones y Administraciones de la Agencia Estatal de Administración Tributaria, y que presten servicio de caja en las mismas, la autoridad gubernativa competente deberá oír previamente a la Delegación o Administración afectada.

Artículo 121. *Requisitos de las cámaras acorazadas y de cajas de alquiler.*

Las cámaras acorazadas de efectivo y de compartimentos de alquiler deberán tener las características y el nivel de resistencia que determine el Ministerio del Interior, y estar provistas de las siguientes medidas de seguridad:

a) Dispositivo mecánico o electrónico que permita el bloqueo de su puerta desde la hora de cierre del establecimiento hasta la primera hora del día siguiente hábil.

b) Sistema de apertura automática retardada, que deberá estar activada durante la jornada laboral, salvo las cámaras de compartimentos de alquiler, que habrán de disponer de sistema electrónico de detección de ataques conectado las veinticuatro horas.

En los supuestos en que las cámaras acorazadas, con la finalidad de permitir el acceso a su interior en caso de emergencia, cuenten con trampones, éstos podrán estar libres de cualquier dispositivo de bloqueo o temporización, siempre que sus llaves sean depositadas para su custodia en otra sucursal próxima de la misma entidad o grupo.

c) Detectores sísmicos, detectores microfónicos u otros dispositivos que permitan detectar cualquier ataque a través de techos, paredes o suelo de las cámaras acorazadas o de las cajas de alquiler.

d) Detectores volumétricos.

e) Mirillas ojo de pez o dispositivos similares, o circuito cerrado de televisión en su interior, conectado con la detección volumétrica o provisto de videosensor, con proyección de imágenes en un monitor visible desde el exterior.

Estas imágenes deberán ser transmitidas a la central de alarmas o, en caso contrario, la entidad habrá de disponer del servicio de custodia de llaves para la respuesta a las alarmas.

Artículo 122. *Cajas fuertes, dispensadores de efectivo y cajeros automáticos.*

1. Las cajas fuertes deberán tener los niveles de resistencia que determine el Ministerio del Interior, y estarán protegidas con los dispositivos de bloqueo y apertura automática retardada, de acuerdo con lo dispuesto en el artículo anterior. Cuando su peso sea inferior a 2.000 kilogramos, estarán, además, ancladas, de manera fija, en estructuras de hormigón armado, al suelo o al muro.

2. Para el funcionamiento del establecimiento u oficina, las cajas auxiliares, además del cajón donde se deposita, en su caso, el efectivo necesario para realizar las operaciones, estarán provistas de elementos con posibilidad de depósito de efectivo en su interior, de forma que quede sometido necesariamente a apertura retardada para su extracción.

3. Los dispensadores de efectivo habrán de estar construidos con materiales de la resistencia que determine el Ministerio del Interior, debiendo estar conectados a la central de alarmas durante el horario de atención al público.

A estos efectos, se consideran dispensadores de efectivo los que, estando provistos de sistema de apertura automática retardada y posibilidad para admitir ingresos, permitan la dispensación automática de efectivo contra cuentas corrientes, contables o libretas de ahorro, libremente, hasta la cantidad que determine el Ministerio del Interior.

Cuando en un establecimiento u oficina todas las cajas auxiliares sean sustituidas por dispensadores de efectivo, no serán precisas las instalaciones a que se refiere el artículo 120.1.d) y e) de este Reglamento. No obstante, podrá disponerse de cajas auxiliares para su utilización en caso de avería de los dispensadores de efectivo.

4. Los cajeros automáticos deberán estar protegidos con las siguientes medidas de seguridad:

1.º Cuando se instalen en el vestíbulo del establecimiento:

a) Puerta de acceso blindada con acristalamiento resistente al menos al impacto manual del nivel que se determine, y dispositivo interno de bloqueo.

b) Dispositivo de apertura automática retardada en la puerta de acceso al depósito de efectivo, que podrá ser desactivado, durante las operaciones de carga, por los vigilantes de seguridad encargados de dichas operaciones, previo aviso, en su caso, al responsable del control de los sistemas de seguridad.

c) Detector sísmico en la parte posterior.

2.º Cuando se instalen en fachada o dentro del perímetro interior de un inmueble, las medidas establecidas en los párrafos b) y c) anteriores.

3.º Cuando se instalen en el interior de edificios, locales o inmuebles, siempre que éstos se encuentren dotados de vigilancia permanente con armas, los cajeros automáticos quedan exceptuados del cumplimiento de las anteriores medidas de seguridad, y únicamente se exigirá que estén anclados al suelo o al muro cuando su peso sea inferior a 2.000 kilogramos.

5. Si los cajeros automáticos se instalaran en espacios abiertos, y no formaran parte del perímetro de un edificio, deberán disponer de cabina anclada al suelo, de las características que se determinen, y estar protegidos con las medidas a que se refiere el apartado 1.o anterior.

Artículo 123. *Planos de planta.*

Los Bancos, Cajas de Ahorro y demás entidades de crédito mantendrán en las oficinas centrales los planos de planta actualizados de todas sus oficinas, descriptivos de la distribución de las distintas dependencias y de las instalaciones de seguridad de los diferentes servicios, e informes técnicos sobre la naturaleza de los materiales utilizados en su construcción. A requerimiento de las unidades de las Fuerzas y Cuerpos de Seguridad, les facilitarán copia de dichos planos por el procedimiento más rápido disponible.

Artículo 124. *Oficinas de cambio de divisas y módulos transportables.*

1. Los establecimientos u oficinas pertenecientes a entidades de crédito u otras mercantiles, dedicadas exclusivamente al cambio de divisas, estacional o permanentemente, dispondrán como mínimo de las medidas de seguridad previstas en el artículo 132 de este Reglamento para las Administraciones de Loterías y Apuestas Mutuas.

2. Los bancos móviles o módulos transportables, utilizados por las entidades de crédito como establecimientos u oficinas, deberán reunir, al menos, las siguientes medidas de seguridad:

a) Protección de la zona destinada al recinto de caja y puertas de acceso con blindaje de cristal antibala de la categoría y nivel que se determinen, para evitar el ataque al personal que se encuentre en el interior de dicho recinto.

El recinto de caja permanecerá cerrado desde su interior, durante las horas de atención al público, siempre que el personal se encuentre dentro del mismo.

b) Caja fuerte con dispositivo automático de retardo y bloqueo, que deberá estar fijada a la estructura del vehículo del módulo. La caja auxiliar estará provista de cajón de depósito y unida a otro de apertura retardada.

c) Señal luminosa exterior y pulsadores de la misma en el interior.

d) Carteles anunciadores como los previstos en el párrafo f) del artículo 120 de este Reglamento.

e) Servicio propio de vigilantes de seguridad, en el supuesto de que no se cuente con servicio de vigilancia de las Fuerzas y Cuerpos de Seguridad o con servicio de vigilantes de seguridad del inmueble o recinto en que se ubiquen.

3. La autorización de cada unidad o módulo para el funcionamiento de estos establecimientos u oficinas corresponderá al Director general de la Policía o al Gobernador Civil de la provincia, según que el ámbito territorial de actuación sea supraprovincial o provincial, debiendo seguirse el procedimiento regulado en el artículo 136 de este Reglamento. Una copia de la autorización deberá estar depositada en la correspondiente unidad o módulo.

Artículo 125. *Exenciones.*

La Dirección General de la Policía para supuestos que excedan del territorio de una provincia o, en otro caso, el Gobierno Civil podrán eximir a las entidades a que se refiere esta Sección de todas o alguna de las medidas de seguridad que se establecen en los artículos 120 y, en su caso, en el 121, 122 y 124, apartados 1 y 2, a solicitud de la entidad interesada, valorando las circunstancias a que se refiere el artículo 112.1, todos del presente

Reglamento. A tal efecto, el órgano competente recabará el parecer de la representación de los trabajadores.

Artículo 126. *Caja Postal.*

Las normas contenidas en la presente Sección para las entidades de crédito obligarán a la sede y oficinas de la Caja Postal, pero no a las oficinas cuya principal actividad sea la prestación de los servicios públicos de Correos y Telégrafos.

Sección 2.ª Joyerías, platerías, galerías de arte y tiendas de antigüedades

Artículo 127. *Medidas de seguridad aplicables.*

1. En los establecimientos de joyería y platería, así como en aquellos otros en los que se fabriquen o exhiban objetos de tal industria, deberán instalarse, por empresas especializadas y, en su caso, autorizadas, las siguientes medidas de seguridad:

a) Caja fuerte o cámara acorazada, con el nivel de resistencia que determine el Ministerio de Justicia e Interior, para la custodia de efectivo y de objetos preciosos, dotada de sistema de apertura automática retardada, que deberá estar activado durante la jornada laboral, y dispositivo mecánico o electrónico que permita el bloqueo de la puerta, desde la hora de cierre hasta primera hora del día siguiente hábil.

Cuando la caja fuerte tenga un peso inferior a 2.000 kilogramos, deberá estar anclada, de manera fija, en una estructura de hormigón armado, al suelo o al muro.

b) Pulsadores antiatraco u otros medios de accionamiento del sistema de alarma que estarán instalados en lugares estratégicos.

c) Rejas en huecos que den a patios y pasos interiores del inmueble, así como cierres metálicos en el exterior, sin perjuicio del cumplimiento de las condiciones exigidas por las normas de lucha contra incendios.

d) Puerta blindada, con resistencia al impacto manual del nivel que se determine, en todos los accesos al interior del establecimiento, provista de los cercos adecuados y cerraduras de seguridad.

e) Protección electrónica de escaparates, ventanas, puertas y cierres metálicos.

f) Dispositivos electrónicos con capacidad para la detección redundante de la intrusión en las dependencias del establecimiento en que haya efectivo u objetos preciosos.

g) Detectores sísmicos en paredes, techos y suelos de la cámara acorazada o del local en que esté situada la caja fuerte.

h) Conexión del sistema de seguridad con una central de alarmas.

i) Carteles, del tamaño que se determine por el Ministerio de Justicia e Interior, u otros sistemas de información de análoga eficacia, para su perfecta lectura desde el exterior del establecimiento, en los que se haga saber al público las medidas de seguridad que éste posea.

2. Los establecimientos de nueva apertura deberán instalar cristales blindados, del nivel que se determine, en escaparates en los que se expongan objetos preciosos, cuyo valor en conjunto sea superior a 15.000.000 de pesetas. Esta protección también será obligatoria para las ventanas o huecos que den al exterior.

3. Las galerías de arte, tiendas de antigüedades y establecimientos que se dediquen habitualmente a la exhibición o subasta de objetos de joyería o platería, así como de antigüedades u obras de arte, cuyas obras u objetos superen en conjunto el valor que se determine, deberán adoptar las medidas de seguridad que se establecen bajo los párrafos b), c), d), e), f), h) e i) del apartado 1 de este artículo y, además, proteger con detectores sísmicos el techo y el suelo del establecimiento y las paredes medianeras con otros locales o viviendas, así como con acristalamiento blindado del nivel que se fija en el apartado anterior los escaparates de los establecimientos de nueva apertura en que se exhiban objetos por la cuantía en el mismo determinada.

Artículo 128. *Exhibiciones o subastas ocasionales.*

1. Con independencia del cumplimiento de las normas aplicables, las personas o entidades que pretendan exhibir o subastar públicamente objetos de joyería o platería, así como antigüedades u obras de arte, en locales o establecimientos no dedicados habitualmente a estas actividades deberán comunicarlo, con una antelación no inferior a quince días, al Gobernador Civil de la provincia donde vaya a efectuarse la exhibición o subasta.

2. Atendiendo a las circunstancias que concurran en cada caso y a los informes recabados, el Gobernador Civil podrá ordenar a los organizadores la adopción, con carácter previo a las exhibiciones o subastas, de las medidas de vigilancia y seguridad que considere adecuadas.

Artículo 129. *Dispensas.*

1. Teniendo en cuenta el reducido volumen de negocio u otras circunstancias que habrán de ser debidamente acreditadas, los Gobernadores Civiles podrán dispensar de todas o algunas de las medidas de seguridad previstas en el artículo 127 de este Reglamento a los establecimientos cuyos titulares lo soliciten.

2. Si lo estimasen conveniente, dichas autoridades podrán recabar la opinión al respecto de las correspondientes asociaciones empresariales de la provincia y de la representación de los trabajadores.

Sección 3.ª Estaciones de servicio y unidades de suministro de combustibles y carburantes

Artículo 130. *Enumeración de medidas de seguridad.*

1. Las estaciones de servicio y unidades de suministro de combustibles y carburantes dispondrán de una caja fuerte con el nivel de resistencia que determine el Ministerio de Justicia e Interior, con sistema o mecanismo que impida la extracción del dinero a través de la abertura destinada a su introducción en la caja, y dos cerraduras protegidas. La caja estará empotrada en una estructura de hormigón armado, preferentemente en el suelo.

2. Una de las llaves de la caja fuerte estará en poder del encargado del negocio u otro empleado y la otra en posesión del propietario o persona responsable de la recogida de los fondos, sin que en ningún caso pueda coincidir la custodia de ambas llaves en la misma persona, ni en personas que trabajen juntas.

3. A fin de permitir las devoluciones y cambios necesarios, cada empleado de las estaciones de servicio y unidades de suministro de combustibles y carburantes sólo podrá tener en su poder, o, en el caso de autoservicio, en la caja registradora, la cantidad de dinero que fije el Ministerio de Justicia e Interior.

4. Las estaciones y unidades de suministro podrán disponer, advirtiéndolo al público usuario mediante carteles situados en lugares visibles, que sólo se despachará combustible por cantidades determinadas de dinero, de forma que puedan ser abonadas por su importe exacto sin necesidad de efectuar cambios.

5. En los casos en los que el volumen económico, la ubicación de las estaciones de servicio o, en general, su vulnerabilidad lo requiera, los Gobernadores Civiles podrán imponer la obligación de las empresas titulares de adoptar alguno de los servicios o sistemas de seguridad establecidos en el artículo 112 de este Reglamento.

6. Será de aplicación a las estaciones de servicio y unidades de suministro de combustibles y carburantes lo dispuesto sobre dispensas en el artículo 129.1 de este Reglamento.

Sección 4.ª Oficinas de farmacia, Administraciones de Lotería, Despachos de Apuestas Mutuas y establecimientos de juego

Artículo 131. *Oficinas de farmacia.*

1. Todas las oficinas de farmacia deberán contar con un dispositivo de tipo túnel, bandeja de vaivén o bandeja giratoria con seguro, que permita adecuadamente las dispensaciones a los clientes sin necesidad de que éstos penetren en el interior.

2. La utilización de esta medida será obligatoria únicamente cuando las farmacias presten servicio nocturno o de urgencia.

Artículo 132. *Administraciones de Lotería y Despachos de Apuestas Mutuas.*

1. Las Administraciones de Lotería y los Despachos Integrales de Apuestas Mutuas Deportivo-Benéficas dispondrán de un recinto cerrado en el que existirá una caja fuerte de las características determinadas en el artículo 127.1.a) del presente Reglamento en la que se custodiarán los efectos y el dinero en metálico.

2. La parte del recinto destinada al público estará totalmente separada, por elementos o materiales de blindaje del nivel que se determine, de la zona reservada a los empleados que realicen transacciones con el público, la cual estará permanentemente cerrada desde su interior y dotada de dispositivos que impidan el ataque a dichos empleados.

3. Las transacciones con el público se harán a través de ventanillas con cualquiera de los dispositivos enumerados en el apartado 1 del artículo anterior.

4. Independientemente de las mencionadas medidas de seguridad, el Gobernador Civil de la provincia, en los casos a que se refiere el artículo 130.5 de este Reglamento, podrá obligar a los titulares de estos establecimientos a la adopción de los sistemas de seguridad a que se refieren los párrafos c) y d) del artículo 112, también del presente Reglamento.

Artículo 133. *Locales de juegos de azar.*

1. Las medidas de seguridad establecidas en los apartados 1 y 2 del artículo anterior serán aplicables asimismo a los casinos de juego.

2. A las salas de bingo autorizadas para más de ciento cincuenta jugadores, así como a los salones de máquinas de juego autorizados para más de setenta y cinco máquinas de juego, les será de aplicación la medida de seguridad regulada en los apartados 1 y 2 del artículo 130 de este Reglamento.

Artículo 134. *Dispensas.*

Será de aplicación a esta sección lo dispuesto sobre dispensas en el artículo 129 del presente Reglamento.

Sección 5.ª Mantenimiento de las medidas de seguridad

Artículo 135. *Revisión. Libro-catálogo.*

1. A los efectos de mantener el funcionamiento de las distintas medidas de seguridad previstas en el presente título y de la consecución de la finalidad preventiva y protectora, propia de cada una de ellas, la dirección de cada entidad o establecimiento obligado a tener medidas de seguridad electrónicas dispondrá la revisión y puesta a punto, trimestralmente, de dichas medidas por personal especializado de empresas de seguridad, o propio si dispone de medios adecuados, no debiendo transcurrir más de cuatro meses entre dos revisiones sucesivas, y anotará las revisiones y puestas a punto que se realicen en un libro-catálogo de las instaladas según el modelo que se apruebe con arreglo a las normas que dicte el Ministerio de Justicia e Interior, concebido de forma que pueda ser objeto de tratamiento y archivo mecanizado e informatizado.

Este libro-catálogo será también obligatorio para las empresas industriales, comerciales o de servicios, conectadas a centrales de alarmas.

2. Cuando las instalaciones permitan la comprobación del estado y del funcionamiento de cada uno de los elementos del sistema desde la central de alarmas, las revisiones preventivas tendrán una periodicidad anual, no pudiendo transcurrir más de catorce meses entre dos sucesivas.

CAPITULO III

Apertura de establecimientos u oficinas obligados a disponer de medidas de seguridad

Artículo 136. *Autorización.*

1. Cuando se pretenda la apertura o traslado de un establecimiento u oficina, cuyos locales o instalaciones hayan de disponer, en todos o algunos de sus servicios, de medidas de seguridad determinadas en este Reglamento, el responsable de aquéllos solicitará la autorización del Delegado del Gobierno, el cual ordenará el examen y comprobación de las medidas de seguridad instaladas y su correcto funcionamiento, a los funcionarios que tienen atribuidas legalmente dichas facultades. Hasta tanto tal comprobación tenga lugar, podrá autorizarse provisionalmente, por la autoridad policial competente, la apertura del establecimiento u oficina por un plazo máximo de tres meses, siempre que se implante transitoriamente el servicio de vigilantes de seguridad con armas.

Cuando se trate de la reforma de un establecimiento u oficina, anteriormente autorizados, que implique la adopción o modificación de medidas de seguridad, bastará la comunicación a las dependencias policiales competentes, para su comprobación.

2. Practicada la inspección sin constatar deficiencias de las medidas de seguridad obligatorias, el establecimiento podrá continuar con sus actividades sin necesidad del servicio de vigilancia armada, hasta que tenga lugar la autorización definitiva, o bien proceder a la apertura provisional, si no lo hubiera hecho con anterioridad, bastando para ello el acta favorable de inspección.

3. De observarse deficiencias en las medidas de seguridad obligatorias, se entregará copia del acta de inspección a la empresa o entidad interesada para la subsanación de aquéllas en el plazo máximo de un mes, debiendo comunicarse la subsanación a la dependencia policial competente a efectos de nueva comprobación. Durante el indicado plazo, el establecimiento podrá permanecer en funcionamiento siempre que cuente con el servicio de vigilantes de seguridad con armas.

Transcurrido dicho plazo sin que la empresa o entidad interesada haya comunicado la subsanación de las deficiencias, se procederá al cierre del establecimiento u oficina hasta que se constate la subsanación de las mismas mediante la correspondiente acta de inspección.

4. En el caso de que la empresa o entidad solicitante no recibiere indicación o comunicación alguna, en el plazo de tres meses siguientes a la fecha de presentación de la solicitud de autorización, o en el de un mes desde la fecha de presentación de la comunicación relativa a la subsanación de deficiencias, podrá entender autorizada la apertura o traslado del establecimiento o aprobada la reforma efectuada.

5. Las medidas de seguridad no obligatorias y las reformas que no afecten a los elementos esenciales del sistema de seguridad, instalados en este tipo de establecimientos u oficinas, habrán de ser comunicadas a las dependencias policiales de los órganos competentes, antes de su entrada en funcionamiento, pero no estarán sujetas a autorización previa.

6. Las previsiones contenidas en el presente artículo serán también aplicables a los cajeros automáticos, en los supuestos de instalación y entrada en funcionamiento, modificación o traslado de los mismos.

TITULO IV

Control e inspección

CAPITULO I

Información y control

Artículo 137. *Competencias y funciones.*

1. Corresponde el ejercicio de la competencia de control para el cumplimiento de la Ley 23/1992, de 30 de julio, de Seguridad Privada, al Ministerio de Justicia e Interior y a los Gobernadores Civiles.

2. Corresponde al Cuerpo Nacional de Policía y, en su caso, al de la Guardia Civil, el cumplimiento de las órdenes e instrucciones que se impartan por los órganos indicados, en el ejercicio de la función de control de las entidades, servicios o actuaciones y del personal y medios en materia de seguridad privada, vigilancia e investigación.

3. Sin perjuicio de lo dispuesto en el apartado anterior, el ejercicio de la función de control de las actuaciones de los guardas particulares del campo, en sus distintas modalidades, corresponde especialmente a la Dirección General de la Guardia Civil.

4. Para el ejercicio de las competencias respectivamente atribuidas por la legislación de seguridad privada a las Direcciones Generales de la Policía y de la Guardia Civil, éstas llevarán ficheros automatizados, destinados a registrar las infracciones cometidas y las sanciones impuestas en los procedimientos sancionadores en que hubieran intervenido en la materia.

Artículo 138. *Documentación anual.*

1. Durante el primer trimestre de cada año, todas las empresas de seguridad remitirán a la Secretaría de Estado de Interior un informe explicativo de las actividades realizadas en el año anterior, en el que constará:

a) La relación de altas y bajas producidas en el personal de seguridad, con indicación de los datos consignados en el correspondiente libro-registro.

b) La relación de servicios realizados, con indicación del nombre de la entidad o persona a la que se prestaron y especificación de la naturaleza de los servicios, determinada con arreglo a la enumeración contenida en el artículo 1 de este Reglamento.

c) El resumen de las comunicaciones efectuadas a las Fuerzas y Cuerpos de Seguridad en relación con la seguridad ciudadana.

d) La relación de auxilios, colaboraciones y entregas de detenidos a las Fuerzas y Cuerpos de Seguridad.

2. Asimismo, las empresas de seguridad remitirán a la Secretaría de Estado de Interior, durante el primer semestre de cada año, el resumen de la cuenta anual, en el que se refleje la situación patrimonial y financiera de la empresa.

Artículo 139. *Comunicación sobre la vigencia del contrato de seguro, aval u otra garantía financiera suscrita para cubrir la responsabilidad.*

1. Anualmente, en el mismo plazo determinado en el apartado 1 del artículo anterior, las empresas de seguridad habrán de presentar, en el registro en que se encontraran inscritas, certificado acreditativo de vigencia del contrato de seguro, aval u otra garantía financiera que hubieran suscrito para cubrir la responsabilidad.

2. La empresa asegurada tiene la obligación de comunicar a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), la rescisión y cualquiera otra de las circunstancias que puedan dar lugar a la terminación del contrato de seguro de responsabilidad civil, aval u otra garantía financiera, al menos con treinta días de antelación a la fecha en que dichas circunstancias hayan de surtir efecto.

3. En todos los supuestos de terminación de la vigencia del contrato de seguro, aval u otra garantía financiera, la empresa deberá concertar oportunamente, de forma que no se produzca solución de continuidad en la cobertura de la responsabilidad, nueva póliza de responsabilidad civil, aval u otra garantía financiera, que cumpla las exigencias establecidas en el artículo 5.1.c).6.º y en el anexo de este reglamento, acreditándolo ante el Registro de Empresas de Seguridad.

Artículo 140. *Comunicación de modificaciones estatutarias.*

1. Cuando las empresas de seguridad revistan la forma de persona jurídica estarán obligadas a comunicar a la Secretaría de Estado de Seguridad todo cambio que se produzca en la titularidad de las acciones, participaciones o aportaciones y los que afecten a su capital social, dentro de los quince días siguientes a su modificación.

2. Asimismo, y en igual plazo, deberán comunicar cualquier modificación de sus Estatutos y toda variación que sobrevenga en la composición personal de sus órganos de administración y dirección.

3. Las comunicaciones a que se refieren los apartados anteriores deberán efectuarse mediante copia autorizada de la correspondiente escritura pública o del documento en que se hubieren consignado las modificaciones.

4. Cuando los cambios implicaran la pérdida de los requisitos de los administradores y directores de las empresas de seguridad, cesarán en sus cargos.

Artículo 141. *Memoria anual de los detectives privados.*

Los detectives privados habrán de presentar en la Secretaría de Estado de Seguridad, dentro del primer trimestre de cada año, una memoria de actividades del año precedente, en la que se hará constar la relación de servicios efectuados, la condición física o jurídica de las personas con las que se concertaron, consignándose en este último caso el sector específico y la actividad concreta de que se trate, la naturaleza de los servicios prestados, los hechos delictivos perseguibles de oficio comunicados como consecuencia de su actuación, y los órganos gubernativos a los que se comunicaron.

Artículo 142. *Perfeccionamiento del sector.*

1. Teniendo en cuenta la información reunida anualmente a través del cumplimiento de lo dispuesto en los artículos anteriores y en los restantes del presente Reglamento, el Ministerio de Justicia e Interior:

a) Dará cuenta anualmente al Gobierno y a las Cortes Generales sobre el funcionamiento del sector de la seguridad privada.

b) Adoptará o promoverá las medidas de carácter general adecuadas para perfeccionar dicho funcionamiento y para asegurar la consecución de las finalidades de la Ley 23/1992, de 30 de julio, de Seguridad Privada.

2. Corresponde al Ministerio de Justicia e Interior, a través de la Dirección General de la Policía, la planificación, información, asesoramiento y coordinación de la seguridad de las personas, edificios, instalaciones, actividades y objetos de especial interés, en el ámbito de la Administración General del Estado y de las entidades de Derecho Público vinculadas o dependientes de ella.

CAPITULO II

Inspección

Artículo 143. *Acceso de los funcionarios.*

1. Los libros-registro de las empresas de seguridad y de los detectives privados determinados en el presente Reglamento estarán a disposición de los miembros del Cuerpo Nacional de Policía, encargados de su control, para las inspecciones que deban realizar.

2. Las empresas y el personal de seguridad privada de las mismas facilitarán el acceso de los funcionarios de las Fuerzas y Cuerpos de Seguridad competentes a los armeros, al

objeto de que puedan realizar las comprobaciones pertinentes sobre los propios armeros y las armas que contengan.

3. Las empresas de depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y objetos valiosos o peligrosos facilitarán la inspección de la cámara acorazada con el fin de hacer las pertinentes comprobaciones de los datos que figuren en los libros-registro.

4. Del mismo modo, las empresas, entidades y organismos que deban tener instalados dispositivos, sistemas o medidas de seguridad, o que tengan servicios de protección prestados por personal de seguridad, o sistemas de seguridad conectados a centrales de alarma, deberán facilitar el acceso a los miembros de las Fuerzas y Cuerpos de Seguridad encargados de las funciones inspectoras a que se refiere este Reglamento, con objeto de que puedan comprobar en cualquier momento el estado de las instalaciones y su funcionamiento.

Artículo 144. *Inspecciones.*

1. Aparte del desarrollo de los planes de inspección que tengan establecidos, cuando recibieren denuncias sobre irregularidades cometidas por empresas o personal de seguridad, o por centros de formación o su personal, los servicios policiales de inspección y control procederán a la comprobación de los hechos denunciados y, en su caso, a la apertura del correspondiente procedimiento.

2. Siempre que el personal indicado realice una inspección de empresas de seguridad, de establecimientos públicos o privados, o de despachos de los detectives privados:

a) Diligenciará los libros revisados, haciendo constar las deficiencias o anomalías que observare.

b) Efectuará las comprobaciones precisas para la constatación del contenido reflejado en los libros, debiendo las empresas y el personal de seguridad colaborar con tal objeto.

c) De cada inspección, extenderá el acta correspondiente, facilitando una copia al responsable del establecimiento.

3. Los actos de inspección, que se contraerán a las medidas, medios y actividades de seguridad privada, podrán desarrollarse, indistintamente:

a) En la sede social de la empresa, delegaciones, oficinas, locales, despachos, o lugares anejos a éstos, en los que se desarrollen actividades de seguridad privada o relacionadas con ésta.

b) En los inmuebles, espacios o lugares en donde se presten servicios de seguridad privada.

CAPITULO III

Medidas cautelares

Artículo 145. *Ocupación o precinto.*

Los funcionarios policiales competentes podrán acordar, inmediata y excepcionalmente, la medida cautelar de ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción, en supuestos de grave riesgo o peligro inminente para las personas o bienes, debiendo, para el mantenimiento de la medida, ser ratificada por las autoridades sancionadoras competentes.

Artículo 146. *Retirada de armas.*

Con independencia de las responsabilidades penales o administrativas a que hubiere lugar, los funcionarios policiales competentes se harán cargo de las armas y darán cumplimiento a lo dispuesto en el artículo 148.2 del Reglamento de Armas, sobre depósito de las que se porten o utilicen ilegalmente, en los siguientes casos:

a) Si detectaren la prestación de servicios por personal de seguridad privada con armas, cuando debieran prestarse sin ellas.

b) Cuando el personal de seguridad privada porte armas fuera de los lugares o de las horas de servicio, sin la oportuna autorización en los casos previstos en el presente Reglamento.

Artículo 147. *Suspensión de servicios.*

Cuando los funcionarios policiales competentes observaren la prestación de servicios de seguridad privada o la utilización de medios materiales o técnicos que puedan causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana, suspenderán su prestación, debiendo tal decisión ser ratificada por el Secretario de Estado de Interior o por los Gobernadores Civiles en el plazo de setenta y dos horas.

TITULO V

Régimen sancionador

CAPITULO I

Cuadro de infracciones

Sección 1.ª Empresas de seguridad

Artículo 148. *Infracciones muy graves.*

Las empresas podrán incurrir en las siguientes infracciones muy graves:

1. La prestación de servicios de seguridad a terceros, careciendo de la autorización necesaria, incluyendo:

a) La prestación de servicios de seguridad sin haber obtenido la inscripción y la autorización de entrada en funcionamiento para la clase de servicios o actividades de que se trate.

b) La continuación de la prestación de servicios en caso de cancelación de la inscripción o de rescisión del contrato de seguro, aval u otra garantía equivalente, sin concertar otra nueva otra nueva dentro del plazo reglamentario.

c) La subcontratación de los servicios y actividades de seguridad privada con empresas que no dispongan de la correspondiente habilitación o reconocimiento necesarios para el servicio o actividad de que se trate, salvo en los supuestos reglamentariamente permitidos.

2. La realización de actividades prohibidas en el artículo 3 de la Ley, sobre conflictos políticos o laborales, control de opiniones, recogida de datos personales con tal objeto, o información a terceras personas sobre sus clientes o su personal, en el caso de que no sean constitutivas de delito.

3. La instalación de medios materiales o técnicos no homologados que sean susceptibles de causar grave daño a las personas o a los intereses generales.

4. La negativa a facilitar, cuando proceda, la información contenida en los libros registros reglamentarios.

5. El incumplimiento de las previsiones normativas sobre adquisición y uso de las armas, así como sobre disponibilidad de armeros, conservación, mantenimiento, buen funcionamiento de las armas y custodia de las mismas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por la Ley, incluyendo:

a) Poseer armas que no sean las reglamentariamente determinadas para el servicio de que se trate.

b) La tenencia de armas careciendo de la guía de pertenencia de las mismas.

c) Adjudicar al personal de seguridad armas que no sean las reglamentariamente establecidas para el servicio.

d) La negligencia en la custodia de armas, que pueda provocar su sustracción, robo o extravío.

e) Carecer de armero con la correspondiente homologación o no hacer uso del mismo, en los casos en que esté exigido en el presente Reglamento.

f) La realización de los ejercicios de tiro obligatorios por el personal de seguridad sin la presencia o sin la dirección del instructor de tiro o, en su caso, del jefe de seguridad, o incumpliendo lo dispuesto al efecto en el artículo 84.2 de este Reglamento.

g) Proveer de armas a personal que carezca de la licencia reglamentaria.

6. La realización de servicios de seguridad con armas fuera de los casos previstos en la Ley y en el presente Reglamento, así como encargar servicios con armas a personal que carezca de la licencia reglamentaria.

7. La negativa a prestar auxilio o colaboración con las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos, en el descubrimiento y detención de los delincuentes o en la realización de las funciones inspectoras o de control que les correspondan, incluyendo:

a) La falta de comunicación oportuna a las Fuerzas y Cuerpos de Seguridad de informaciones relevantes para la prevención, mantenimiento o restablecimiento de la seguridad ciudadana.

b) La falta de comunicación oportuna de los hechos delictivos de que tuvieren conocimiento en el desarrollo de sus actividades.

c) La negativa a facilitar a los funcionarios competentes los contratos, libros-registro u hojas de ruta reglamentarios, que contengan datos relacionados con los servicios de seguridad privada.

d) La negativa a facilitar a dichos funcionarios el acceso a los lugares donde se lleven a cabo actividades de seguridad privada, o se presten servicios de esta naturaleza, excepto a los domicilios particulares.

e) Impedir o dificultar de cualquier modo el control de la prestación de servicios de seguridad, cuando se establezcan sistemas informáticos de comunicación.

8. La comisión de una tercera infracción grave en el período de un año.

Artículo 149. *Infracciones graves.*

Las empresas de seguridad podrán incurrir en las siguientes infracciones graves:

1. La instalación de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

2. La realización de servicios de transportes con vehículos que no reúnan las características reglamentarias, incluyendo:

a) La utilización de vehículos con distintivos o características semejantes a los de las Fuerzas Armadas o a los de las Fuerzas y Cuerpos de Seguridad o con lanzadestellos o sistemas acústicos que les estén prohibidos.

b) La realización de los servicios de transporte o distribución sin que los vehículos cuenten con la dotación reglamentaria de vigilantes de seguridad o, en su caso, sin la protección necesaria.

3. La realización de funciones que excedan de la habilitación obtenida o reconocida por la empresa de seguridad o por el personal a su servicio, o fuera del lugar o ámbito territorial correspondiente, así como la retención de la documentación personal; la realización de servicios en polígonos industriales y urbanizaciones sin haber obtenido la autorización expresa de la Delegación o Subdelegación del Gobierno o del órgano correspondiente de la comunidad autónoma competente, y la subcontratación de servicios de seguridad con empresas inscritas, pero no habilitadas o reconocidas para el ámbito territorial correspondiente al lugar de realización del servicio o actividad subcontratados.

4. La realización de los servicios de seguridad sin formalizar o sin comunicar a la autoridad competente la celebración de los correspondientes contratos, incluyendo:

a) La realización de servicios de protección personal, careciendo de la autorización a que se refieren los artículos 27 y siguientes de este Reglamento, fuera del plazo establecido o al margen de las condiciones impuestas en la autorización.

b) La falta de comunicación de los contratos, o, en su caso, de las ofertas en que se concreten sus prestaciones, o de las modificaciones de los mismos, a las autoridades competentes ; no hacerlo dentro de los plazos establecidos, o realizarlo sin ajustarse a los modelos o formatos aprobados, y la prestación de los servicios, en circunstancias o condiciones distintas de las previstas en los contratos comunicados.

c) La falta de comunicación a las autoridades competentes, dentro del plazo establecido, de la prestación de servicios urgentes, en circunstancias excepcionales.

5. La utilización en el ejercicio de funciones de seguridad, de personas que carezcan de la nacionalidad, cualificación, acreditación o titulación exigidas, o de cualquier otro de los requisitos necesarios, **incluyendo el de la superación de los correspondientes cursos de actualización y especialización con la periodicidad establecida**, y la utilización de personal habilitado sin la correspondiente comunicación de alta en las empresas, en la forma establecida.

6. El abandono o la omisión injustificados del servicio, dentro de la jornada laboral establecida, por parte de los vigilantes de seguridad y de todo el personal de seguridad privada al que se aplican las normas de los vigilantes.

7. La falta de presentación a la autoridad competente del informe anual de actividades, en la forma y plazo prevenidos o con omisión de las informaciones requeridas legal y reglamentariamente.

8. No transmitir a las Fuerzas y Cuerpos de Seguridad las señales de alarma que se registren en las centrales privadas, transmitir las señales con retraso injustificado o comunicar falsas incidencias, por negligencia, deficiente funcionamiento o falta de verificación previa, incluyendo:

a) El funcionamiento deficiente de las centrales de alarmas por carecer del personal preciso.

b) La transmisión de alarmas a los servicios policiales sin verificarlas previa y adecuadamente.

c) La transmisión de falsas alarmas a las Fuerzas y Cuerpos de Seguridad por falta de adopción de las precauciones necesarias para evitarlas.

d) La falta de subsanación de las deficiencias que den lugar a falsas alarmas, cuando se hubiere sido requerido para ello, y la de desconexión del sistema que hubiere sido reglamentariamente ordenada.

9. La comisión de una tercera infracción leve en el período de un año.

> Téngase en cuenta que se anula el inciso destacado en el apartado 5 por Sentencia del TS de 15 de enero de 2009. Ref. BOE-A-2009-3500.

Artículo 150. *Infracciones leves.*

Las empresas de seguridad podrán incurrir en las siguientes infracciones leves:

1. La entrada en funcionamiento de las empresas de seguridad sin dar cuenta de ello a los servicios policiales competentes, salvo que constituya infracción grave o muy grave.

2. La apertura de delegaciones o sucursales sin obtener la autorización necesaria del órgano competente.

3. La omisión del deber de abrir sucursales o delegaciones en los supuestos prevenidos en los apartados 2 y 3 del artículo 17.

4. La publicidad de la empresa sin estar inscrita y autorizada, y la realización de publicidad de las actividades y servicios o la utilización de documentos o impresos en sus comunicaciones, sin hacer constar el número de registro de la empresa.

5. La falta de presentación anual, dentro del plazo establecido, del certificado acreditativo de la vigencia del contrato de seguro, aval u otra garantía equivalente.

6. La falta de comunicación a la autoridad competente, en el plazo y en la forma prevenidos, de los cambios que afecten a la titularidad de las acciones o participaciones en el capital o a la composición personal de los órganos de administración, y de cualquier variación en los órganos de dirección de la sociedad.

7. La falta de comunicación a la autoridad competente de la información prevenida durante la prestación de servicios de protección personal o la relativa a la finalización del servicio.

8. La omisión del deber de reserva en la programación, itinerario y realización de los servicios relativos al transporte y distribución de objetos valiosos o peligrosos.

9. La realización de las operaciones de transporte, carga o descarga de objetos valiosos o peligrosos en forma distinta de la prevenida o sin adoptar las precauciones necesarias para su seguridad.

10. La realización de los servicios sin asegurar la comunicación entre la sede de la empresa y el personal que los desempeñe cuando fuere obligatoria.

11. La omisión de las prevenciones o precauciones reglamentarias en el transporte de objetos valiosos por vía marítima o aérea.

12. La omisión de los proyectos de instalación, previos a la instalación de medidas de seguridad; de las comprobaciones necesarias, o de la expedición del correspondiente certificado que garantice que las instalaciones de seguridad cumplen las exigencias reglamentarias.

13. La falta de realización de las revisiones obligatorias de las instalaciones de seguridad sin cumplir la periodicidad establecida o con personal que no reúna la cualificación requerida.

14. La carencia de servicio técnico necesario para arreglar las averías que se produzcan en los aparatos, dispositivos o sistemas de seguridad obligatorios; o tenerlo sin la capacidad o eficacia adecuadas.

15. El incumplimiento de la obligación de entregar el manual de la instalación o el manual de uso del sistema de seguridad o facilitarlos sin reunir las exigencias reglamentarias.

16. La prestación de servicios de custodia de llaves, careciendo de armero o de caja fuerte o sin cumplir las precauciones prevenidas al efecto.

17. La actuación del personal de seguridad sin la debida uniformidad o los medios que reglamentariamente sean exigibles.

18. La omisión del deber de adaptar los libros-registro reglamentarios a las normas reguladoras de sus formatos o modelos ; del de llevarlos regularmente y al día, o del de cumplir las normas de funcionamiento del sistema o sistemas de información, comunicación o certificación que se determinen.

19. En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por la Ley de Seguridad Privada o por el presente Reglamento, siempre que no constituya delito o infracción grave o muy grave.

Sección 2.ª Personal de seguridad privada

Artículo 151. *Infracciones muy graves.*

El personal que desempeñe funciones de seguridad privada, podrá incurrir en las siguientes infracciones muy graves:

1. La prestación de servicios de seguridad a terceros por parte de personal no integrado en empresas de seguridad, careciendo de la habilitación necesaria, lo que incluye:

a) Prestar servicios de seguridad privada sin haber obtenido la tarjeta de identidad profesional correspondiente o sin estar inscrito, cuando proceda, en el pertinente registro.

b) Ejercer funciones de seguridad privada distintas de aquellas para las que se estuviere habilitado.

c) Abrir despachos de detective privado o dar comienzo a sus actividades sin estar inscrito en el reglamentario registro o careciendo de la tarjeta de identidad profesional.

d) Prestar servicios como detective asociado o dependiente sin estar inscrito en el correspondiente registro o sin tener la tarjeta de identidad profesional.

e) La utilización por los detectives privados de los servicios de personal no habilitado para el ejercicio de funciones de investigación.

2. El incumplimiento de las previsiones contenidas en la Ley 23/1992, de 30 de julio, de Seguridad Privada, y en el presente Reglamento sobre tenencia de armas fuera del servicio y sobre su utilización, incluyendo:

a) La prestación con armas de servicios de seguridad para los que no estuviese legal o reglamentariamente previsto su uso.

b) Portar sin autorización específica las armas fuera de las horas o de los lugares de prestación de los servicios o no depositarlas en los armeros correspondientes.

c) Descuidar la custodia de sus armas o de las documentaciones de éstas, dando lugar a su extravío, robo o sustracción.

d) No comunicar oportunamente a las Fuerzas y Cuerpos de Seguridad el extravío, destrucción, robo o sustracción del arma asignada.

e) Prestar con arma distinta de la reglamentaria los servicios que puedan ser realizados con armas.

f) Retener las armas o sus documentaciones cuando causaren baja en la empresa a la que pertenecieren.

3. La falta de reserva debida sobre las investigaciones que realicen los detectives privados o la utilización de medios materiales o técnicos que atenten contra el derecho el honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones, incluyendo la facilitación de datos sobre las investigaciones que realicen a personas distintas de las que se las encomienden.

4. La condena mediante sentencia firme por un delito doloso cometido en el ejercicio de sus funciones.

5. La negativa a prestar auxilio o colaboración con las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos, en el descubrimiento y detención de los delincuentes o en la realización de las funciones inspectoras o de control que les correspondan, incluyendo:

a) La falta de comunicación a las Fuerzas y Cuerpos de Seguridad de informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de que tuvieren conocimiento en el ejercicio de sus funciones.

b) Omitir la colaboración que sea requerida por las Fuerzas y Cuerpos de Seguridad en casos de suspensión de espectáculos, desalojo o cierre de locales y en cualquier otra situación en que sea necesaria para el mantenimiento o el restablecimiento de la seguridad ciudadana.

c) La omisión del deber de realizar las identificaciones pertinentes, cuando observaren la comisión de delitos, o del de poner a disposición de las Fuerzas y Cuerpos de Seguridad a sus autores o a los instrumentos o pruebas de los mismos.

d) No facilitar a la Administración de Justicia o a las Fuerzas y Cuerpos de Seguridad las informaciones de que dispusiesen y que les fueren requeridas en relación con las investigaciones que estuviesen realizando.

6. La comisión de una tercera infracción grave en el período de un año.

Artículo 152. *Infracciones graves.*

El personal que desempeñe funciones de seguridad privada podrá incurrir en las siguientes infracciones graves:

1. La realización de funciones o servicios que excedan de la habilitación obtenida, incluyendo:

a) Abrir despachos delegados o sucursales los detectives privados sin reunir los requisitos reglamentarios, sin comunicarlo a la autoridad competente o sin acompañar los documentos necesarios.

b) La realización por los detectives privados, de funciones que no les corresponden, y especialmente la investigación de delitos perseguibles de oficio.

c) Realizar los vigilantes de seguridad actividades propias de su profesión fuera de los edificios o inmuebles cuya vigilancia y protección tuvieran encomendada, salvo en los casos en que estuviere reglamentariamente prevista.

d) El desempeño de las funciones de escolta privado excediéndose de las finalidades propias de su protección o la identificación o detención de personas salvo que sea imprescindible para la consecución de dichas finalidades.

e) Simultanear, en la prestación del servicio, las funciones de seguridad privada con otras distintas, o ejercer varias funciones de seguridad privada que sean incompatibles entre sí.

2. El ejercicio abusivo de sus funciones en relación con los ciudadanos, incluyendo:

a) La comisión de abusos, arbitrariedades o violencias contra las personas.

b) La falta de proporcionalidad en la utilización de sus facultades o de los medios disponibles.

3. No cumplir, en el ejercicio de su actuación profesional, el deber de impedir o evitar prácticas abusivas, arbitrarias o discriminatorias, que entrañen violencia física o moral, en el trato a las personas.

4. La falta de respeto al honor o a la dignidad de las personas.

5. La realización de actividades prohibidas sobre conflictos políticos y laborales, control de opiniones o comunicación de información a terceros sobre sus clientes, personas relacionadas con ellos, o sobre los bienes y efectos que custodien, incluyendo:

a) El interrogatorio de los detenidos o la obtención de datos sobre los ciudadanos a efectos de control de opiniones de los mismos.

b) Facilitar a terceros información que conozcan como consecuencia del ejercicio de sus funciones.

6. El ejercicio de los derechos sindicales o laborales al margen de lo dispuesto al respecto para los servicios públicos, en los supuestos a que se refiere el artículo 15 de la Ley.

7. La falta de presentación al Ministerio de Justicia e Interior, del informe de actividades de los detectives privados, en la forma y plazo prevenidos o su presentación careciendo total o parcialmente de las informaciones necesarias.

8. La falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

9. La comisión de una tercera infracción leve en el período de un año.

Artículo 153. *Infracciones leves.*

El personal que desempeñe funciones de seguridad privada podrá incurrir en las siguientes infracciones leves:

1. La actuación sin la debida uniformidad o medios que reglamentariamente sean exigibles, por parte del personal no integrado en empresas de seguridad.

2. El trato incorrecto o desconsiderado con los ciudadanos con los que se relacionen en el ejercicio de sus funciones.

3. No comunicar oportunamente al registro las variaciones de los datos registrales de los detectives titulares o detectives asociados o dependientes.

4. La publicidad de los detectives privados careciendo de la habilitación necesaria, y la realización de la publicidad o la utilización de documentos o impresos, sin hacer constar el número de inscripción en el registro.

5. No llevar los detectives privados el libro-registro prevenido, no llevarlo con arreglo a las normas reguladoras de modelos o formatos, o no hacer constar en él los datos necesarios.

6. No comunicar oportunamente a las Fuerzas y Cuerpos de Seguridad el extravío, destrucción, robo o sustracción de la documentación relativa a las armas que tuvieran asignadas.

7. La falta de comunicación oportuna por parte del personal de seguridad privada de las ausencias del servicio o de la necesidad de ausentarse, a efectos de sustitución o relevo.

8. La utilización de perros en la prestación de los servicios, sin cumplir los requisitos o sin tener en cuenta las precauciones prevenidas al efecto.

9. No utilizar los uniformes y distintivos, cuando sea obligatorio, o utilizarlos fuera de los lugares o de las horas de servicio.

10. La delegación por los jefes de seguridad de facultades no delegables o hacerlo en personas que no reúnan los requisitos reglamentarios.

11. Desatender sin causa justificada las instrucciones de las Fuerzas y Cuerpos de Seguridad en relación con las personas o bienes objeto de su vigilancia y protección.

12. No mostrar su documentación profesional a los funcionarios policiales o no identificarse ante los ciudadanos con los que se relacionasen en el servicio, si fuesen requeridos para ello.

13. En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por la Ley de Seguridad Privada o por el presente Reglamento, siempre que no constituyan delito o infracción grave o muy grave, incluyendo la no realización de los correspondientes cursos de actualización y especialización o no hacerlos con la periodicidad establecida.

Sección 3.ª Usuarios de los servicios de seguridad

Artículo 154. *Infracciones.*

Las personas físicas o jurídicas, entidades y organismos que utilicen medios o contraten la prestación de servicios de seguridad podrán incurrir en las infracciones siguientes:

1. Infracciones muy graves: la utilización de aparatos de alarmas, dispositivos o sistemas de seguridad no homologados que fueren susceptibles de causar graves daños a las personas o a los interesados generales.

2. Infracciones graves:

a) La utilización de aparatos de alarma o dispositivos de seguridad que no se hallen debidamente homologados.

b) La contratación o utilización de los servicios de empresas carentes de la habilitación específica necesaria para el desarrollo de los servicios de seguridad privada, a sabiendas de que no reúnen los requisitos legales al efecto.

3. Infracciones leves:

a) La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen o su funcionamiento con daños o molestias para terceros.

b) La instalación de marcadores automáticos para transmitir alarmas directamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

c) La contratación o utilización de personal de seguridad que carezca de la habilitación específica necesaria, a sabiendas de que no reúne los requisitos legales.

Sección 4.ª Infracciones al régimen de medidas de seguridad

Artículo 155. *Infracciones.*

1. Los titulares de las empresas, entidades y establecimientos obligados por el presente Reglamento o por decisión de la autoridad competente a la adopción de medidas de seguridad para prevenir la comisión de actos delictivos podrán incurrir en las siguientes infracciones de acuerdo con lo dispuesto en los artículos 23.n), 24 y 26.f), h) y j), de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana:

1.º Infracciones muy graves: podrán ser consideradas infracciones muy graves las infracciones graves, teniendo en cuenta la entidad del riesgo producido o del perjuicio causado.

2.º Infracciones graves:

a) Proceder a la apertura de un establecimiento u oficina o iniciar sus actividades antes de que el órgano competente haya concedido la necesaria autorización.

b) Proceder a la apertura o ejercer las actividades propias del establecimiento u oficina antes de que las medidas de seguridad obligatorias hayan sido adoptadas y funcionen adecuadamente.

c) Mantener abierto el establecimiento u oficina sin que las medidas de seguridad reglamentariamente exigidas funcionen, o sin que lo hagan correcta y eficazmente.

3.º Infracciones leves:

a) Las irregularidades en la cumplimentación de los registros prevenidos.

b) La omisión de los datos o comunicaciones obligatorios dentro de los plazos prevenidos.

c) La desobediencia de los mandatos de la autoridad o de sus agentes, dictados en directa aplicación de lo prevenido en la Ley Orgánica 1/1992, de 21 de febrero, desarrollado, en su caso, reglamentariamente sobre medidas de seguridad en establecimientos e instalaciones, siempre que no constituya infracción penal.

d) La desobediencia de los mandatos de la autoridad o de sus agentes, dictados en aplicación de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, siempre que no constituya infracción penal.

2. También, de acuerdo con lo dispuesto en los artículos 23.n), 24 y 26.h) y j) de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, el personal de las empresas, entidades o establecimientos obligados a la adopción de medidas de seguridad para prevenir la comisión de actos delictivos, podrá incurrir en las siguientes infracciones, sin perjuicio de la responsabilidad en que incurran por los mismos hechos las empresas, entidades o establecimientos indicados:

1. Infracciones muy graves: podrán ser consideradas muy graves las infracciones graves, teniendo en cuenta la entidad del riesgo producido o del perjuicio causado, o el hecho de que se hubiesen producido con violencia o amenazas colectivas.

2. Infracciones graves: la realización de los actos que tengan prohibidos o la omisión de los que les corresponda realizar, dando lugar a que las medidas de seguridad obligatorias no funcionen o lo hagan defectuosamente.

3. Infracciones leves: las definidas en el apartado 1.3.º del presente artículo, bajo los párrafos c) y d).

CAPITULO II

Procedimiento

Artículo 156. *Disposición general.*

Al procedimiento sancionador le será de aplicación lo dispuesto con carácter general en el Reglamento de Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto, con las especialidades previstas en los artículos siguientes.

Artículo 157. *Iniciación.*

Tienen competencia para ordenar la incoación del procedimiento sancionador y para adoptar, si procede, las medidas cautelares que determina el artículo 35 de la Ley de Seguridad Privada:

a) El Ministro de Justicia e Interior, el Secretario de Estado de Interior, el Director general de la Policía y los Gobernadores Civiles, con carácter general, y el Director general de la Guardia Civil respecto a las infracciones cometidas por guardas particulares del campo en sus distintas modalidades.

b) Para las infracciones leves:

1.º Las Jefaturas Superiores o Comisarías Provinciales de Policía.

2.º Las Comandancias de la Guardia Civil respecto a las cometidas por los guardas particulares del campo en sus
distintas modalidades.

c) Todos los órganos mencionados, en materias relacionadas con medidas de seguridad, según el ámbito geográfico en que hubieran sido cometidas.

Artículo 158. *Organos instructores.*

1. La instrucción de los procedimientos sancionadores por faltas muy graves y graves corresponderá a los Gobiernos Civiles, salvo cuando corresponda a los Gobernadores Civiles el ejercicio de la potestad sancionadora.
2. La instrucción de los procedimientos sancionadores, en los supuestos no comprendidos en el apartado anterior, corresponderá a las Comisarías Provinciales de Policía y, en su caso, a las Comandancias de la Guardia Civil.

Artículo 159. *Informe.*

En los procedimientos por faltas muy graves o graves, antes de formular la propuesta de resolución, el órgano instructor, en su caso, remitirá copia del expediente instruido, e interesará informe a la unidad orgánica central de seguridad privada de la Dirección General de la Policía, que habrá de emitirlo en un plazo de quince días.

Artículo 160. *Fraccionamiento del pago.*

1. Cuando la sanción sea de naturaleza pecuniaria, la autoridad que la impuso podrá acordar, previa solicitud fundada del interesado, el fraccionamiento del pago, dentro del plazo de treinta días previsto legalmente.
2. Si se acordase el fraccionamiento del pago, éste se efectuará mediante el abono de la sanción en dos plazos, por un importe de un 50 por 100 de la misma en cada uno de ellos.

Artículo 161. *Publicación de sanciones.*

Cuando la especial transcendencia o gravedad de los hechos, el número de personas afectadas o la conveniencia de su conocimiento por los ciudadanos lo hagan aconsejable, las autoridades competentes podrán acordar que se haga pública la resolución adoptada en procedimientos sancionadores por infracciones graves o muy graves.

Disposición adicional primera. *Funciones de las Policías de las Comunidades Autónomas.*

Los órganos correspondientes y, en su caso, las Policías de las Comunidades Autónomas con competencias para la protección de personas y bienes y para el mantenimiento del orden público, con arreglo a lo dispuesto en sus Estatutos de Autonomía y lo previsto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, ejercerán las facultades de autorización, inspección y sanción de las empresas de seguridad que tengan su domicilio legal en el territorio de cada Comunidad Autónoma y el ámbito de actuación limitado al mismo. También les corresponderá la denuncia, y puesta en conocimiento de las autoridades competentes, de las infracciones cometidas por las empresas de seguridad que no tengan su domicilio legal en el territorio de la Comunidad Autónoma o su ámbito de aplicación limitado al mismo. Asimismo, ejercerán las facultades en materia de seguridad privada derivadas de la disposición adicional de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana. En particular, les corresponden las funciones reguladas en los artículos de este Reglamento que seguidamente se determinan:

1.ª Artículo 2.1. El requisito de inscripción debe cumplimentarse en el Registro de la Comunidad Autónoma competente.
2.ª Artículo 5.1. Instrucción y resolución de las distintas fases del procedimiento de habilitación de empresas de seguridad. Conocimiento del propósito de terminación del contrato de seguro de responsabilidad civil.

3.ª Artículo 5.3. Inspección y control en materia de seguridad privada, así como requerimiento de informes sobre las características de los armeros de empresas de seguridad.

4.ª Artículo 7.1 La referencia a la Caja General de Depósitos se entenderá hecha a la caja que determine la comunidad autónoma correspondiente.

5.ª Artículo 12.2. Cancelación de inscripciones de empresas de seguridad.

6.ª Artículos 14.1 y 15. Recepción de informaciones relativas a actividades y al personal de las empresas de seguridad. Y control de comienzo de las actividades de las empresas de seguridad inscritas y autorizadas por la Comunidad Autónoma.

7.ª Artículo 17.1 y 2. Solicitud o conocimiento de la apertura de delegaciones o sucursales de empresas de seguridad.

8.ª Artículos 19.1.a), 20 y 21. Control de prestación de servicios y de los contratos correspondientes.

9.ª Artículo 24. Determinación de servicios en los que las empresas deberán garantizar la comunicación entre sus sedes y el personal que los desempeñe.

10.ª Artículo 27, apartados 3 y 4, y artículo 28 ; artículo 29, y artículo 30, apartados 1, 4 y 5.

11.ª Autorización de actividades de protección de personas, cuando se desarrollen en el ámbito territorial de la Comunidad Autónoma.

12.ª Autorizaciones provisionales de carácter inmediato para la prestación de servicios de protección personal.

13.ª Comunicación de la composición de la escolta, de sus variaciones y de la finalización del servicio, así como comunicación a las Policías de las Comunidades Autónomas de las autorizaciones concedidas, de los datos de las personas protegidas y de los escoltas y del momento de iniciación y finalización del servicio.

Los órganos correspondientes de la Comunidad Autónoma competente darán cuenta oportunamente a la Dirección General de la Policía de las autorizaciones concedidas y de las comunicaciones recibidas, de acuerdo con lo dispuesto en los mencionados artículos 27, 28, 29 y 30.

14.ª Artículo 32.1. Determinación de protección de vehículos no blindados.

15.ª Artículo 36. Supervisión de los transportes de fondos, valores u objetos.

16.ª Artículo 44. Conocimiento de las características del servicio técnico de averías.

17.ª Artículo 50. Requerimiento de subsanación de deficiencias y orden de desconexión del sistema con la central de alarmas.

18.ª Artículo 66.3. Regulación y concesión de distinciones honoríficas.

19.ª Artículo 80.2. Autorización de servicios de seguridad en polígonos industriales o urbanizaciones aisladas.

20.ª Artículo 93.3. Autorización de servicios con armas por guardas particulares del campo cuyas actividades se desarrollen en el ámbito territorial de la Comunidad Autónoma.

21.ª Artículo 96.b) y c). Disposición sobre prestación de servicios bajo la dirección de un jefe de seguridad.

22.ª Artículo 100. Comunicación de altas y bajas de los jefes de seguridad y de los directores de seguridad.

23.ª Artículos 104, 105 y 107. La apertura de despachos de detectives privados y de sus delegaciones y sucursales, así como los actos constitutivos de sociedades de detectives y sus modificaciones, en el territorio de la Comunidad Autónoma deberán ser comunicadas a ésta por la Dirección General de la Policía, tan pronto como figuren regularizados en el correspondiente Registro.

24.ª Artículo 111. Resolución sobre adopción de medidas de seguridad por parte de empresas o entidades industriales, comerciales o de servicios.

25.ª Artículo 112.1. Exigencia a las empresas o entidades para que adopten servicios o sistemas de seguridad.

26.ª Artículo 115. Comunicaciones relativas a la creación de departamentos de seguridad y a la designación de directores de seguridad.

Artículo 115. Solicitudes de creación de departamentos de seguridad.

27.ª Artículo 118. Concesión de dispensas de la implantación o mantenimiento del servicio de vigilantes de seguridad, e inspección por parte de la Policía de la Comunidad Autónoma correspondiente.

28.ª Artículo 120.2, párrafo tercero.

Autorización para la sustitución de medidas de seguridad por la implantación del servicio de vigilantes de seguridad.

29.ª Artículo 124.3. Autorización para el funcionamiento de oficinas de cambio de divisas, bancos móviles y módulos transportables.

30.ª Artículo 125. Concesión de exenciones de implantación de medidas de seguridad.

31.ª Artículo 128. Conocimiento de realización de exhibiciones o subastas de objetos de joyería o platería, así como de antigüedades u obras de arte, así como la imposición de medidas de seguridad.

32.ª Artículo 129. Dispensa de la adopción de medidas de seguridad.

33.ª Artículo 130.5 y 6. Imposición de la obligación de adoptar servicios o sistemas de seguridad a las estaciones de servicio y unidades de suministro de combustibles y carburantes, así como la dispensa de la adopción de medidas de seguridad.

34.ª Artículo 132.4. Adopción de sistemas de seguridad por parte de Administraciones de Lotería y Despachos de Apuestas Mutuas.

35.ª Artículo 136. Comprobaciones, inspecciones y autorizaciones de apertura y traslado de establecimientos u oficinas obligados a disponer de medidas de seguridad, y de instalación, modificación y traslado de cajeros automáticos.

36.ª Artículo 137.1. Competencia de control en materia de seguridad privada.

37.ª Artículo 137.2. Colaboración de la Policía para el ejercicio de la función de control.

38.ª Artículo 137.3. Control de las actuaciones de los guardas particulares del campo.

39.ª Artículo 138. Del informe anual de actividades de las empresas de seguridad que tengan su domicilio social y su ámbito de actuación limitado al territorio de una Comunidad Autónoma competente en la materia, que sea remitido a la Secretaría de Estado de Interior, será enviada copia por dicha Secretaría al órgano correspondiente de la Comunidad Autónoma.

40.ª Artículo 140. Comunicación de modificaciones de empresas de seguridad inscritas en el Registro de la Comunidad Autónoma.

41.ª Artículo 141. De la memoria anual de actividades de los detectives privados con despachos, delegaciones o sucursales sitos exclusivamente en el territorio de una Comunidad Autónoma competente en la materia, que sea remitida a la Secretaría de Estado de Interior, será enviada copia por dicha Secretaría al órgano correspondiente de la Comunidad Autónoma.

42.ª Artículo 143. Disposición de los libros-registro de las empresas de seguridad, y de los detectives privados, y acceso a armeros, cámaras acorazadas e instalaciones de aquéllas ; todo ello a efectos de inspección y control.

43.ª Artículo 145. Adopción de la medida cautelar de ocupación o precinto y ratificación de la misma, en su caso.

44.ª Artículo 147. Suspensión y ratificación de la suspensión, de servicios de seguridad privada o de la utilización de medios materiales o técnicos.

45.ª Artículo 157.2. Competencia para ordenar la incoación de procedimientos sancionadores y para adoptar medidas cautelares en relación con las empresas de seguridad.

46.ª Artículo 158. Competencia para la instrucción de procedimientos sancionadores a las empresas de seguridad.

47.ª Artículos 160 y 162. Competencia para la emisión de informe y para acordar la publicación de la sanción.

Disposición adicional segunda. *Reducción de los mínimos de garantía.*

Las cantidades determinantes de los mínimos de garantía, especificadas en el apartado I del anexo a este Reglamento, cualesquiera que fueren las actividades que realicen o servicios que presten, quedarán reducidas al 50 por 100, cuando se trate de empresas que tengan una plantilla de menos de 50 trabajadores, y durante dos años consecutivos no superen los 601.012,10 euros (100.000.000 de pesetas) de facturación anual.

Disposición derogatoria única.

Queda derogado el apartado 2 del artículo 30 y el apartado 5 del artículo 43 del Reglamento de Seguridad Privada.

Disposición final primera. *Efectos de la falta de resoluciones expresas.*

Las solicitudes de autorizaciones, dispensas y exenciones, así como las de habilitaciones de personal, reguladas en el presente Reglamento se podrán considerar desestimadas y se podrán interponer contra su desestimación los recursos procedentes, si no recaen sobre ellas resoluciones expresas dentro del plazo de tres meses y de la ampliación del mismo, en su caso, salvo que tengan plazos específicos establecidos en el presente Reglamento, a partir de la fecha en que la solicitud haya tenido entrada en cualquiera de los registros del órgano administrativo competente, sin perjuicio de la obligación de las autoridades competentes de resolver expresamente.

Disposición final segunda. *Uso o consumo de productos provenientes de Estados miembros de la Unión Europea.*

Las normas contenidas en el presente Reglamento y en los actos y disposiciones de desarrollo y ejecución del mismo, sobre vehículos y material de seguridad, no impedirán el uso o consumo en España de productos provenientes de otros Estados miembros de la Unión Europea, que respondan, en lo concerniente a la seguridad, a normas equivalentes a las del Estado español, y siempre que ello se haya establecido mediante la realización de ensayos o pruebas de conformidad equivalentes a las exigidas en España.

ANEXO

Requisitos específicos de las empresas de seguridad, según las distintas clases de actividad

I. Requisitos de inscripción y autorización inicial.

1. Vigilancia y protección de bienes, establecimientos, certámenes o convenciones.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes de seguridad.

C) Tercera fase.

a) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características que determine el Ministerio del Interior.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,10 euros por siniestro y año.

c) Tener constituida, en la forma que se determina en el artículo 7 de este reglamento, una garantía de 240.404,84 euros si el ámbito de actuación es estatal y de 48.080,97 euros, más 12.020,24 euros por provincia, si el ámbito de actuación es autonómico.

2. Protección de personas.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los escoltas privados.

C) Tercera fase.

a) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, un armero o caja fuerte de las características que determine el Ministerio del Interior.

b) Tener concertado un seguro de responsabilidad civil, aval u otra garantía financiera, con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.

c) Tener constituida, en la forma determinada en el artículo 7 de este reglamento, una garantía de 240.404,84 euros.

d) Disponer de medios de comunicación suficientes para garantizar la comunicación entre las unidades periféricas móviles y la estación base.

3. Depósito, custodia y tratamiento de objetos valiosos o peligrosos, y custodia de explosivos.

3.1 Objetos valiosos o peligrosos.

A) Fase inicial. Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes que integran el servicio de seguridad.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,42 euros por siniestro y año.

b) Tener constituida una garantía de 240.404,84 euros si se trata de empresa de ámbito estatal, y de 60.101,21 euros, más 12.020,4 euros por provincia, si es empresa de ámbito autonómico.

c) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características determinadas por el Ministerio del Interior.

d) Tener instalada cámara acorazada y locales anejos de las características y con el sistema de seguridad que determine el Ministerio del Interior.

Los requisitos relativos a cámara acorazada, vigilantes de seguridad que integran el servicio de seguridad y armero o caja fuerte, se exigirán por cada inmueble que destine la empresa a esta actividad.

3.2 Explosivos.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Servicio de seguridad compuesto por un jefe de seguridad y una dotación de, al menos, cinco vigilantes de explosivos, por cada depósito comercial o de consumo de explosivos en el que se preste servicio de custodia.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.

b) Tener constituida una garantía de 120.202,42 euros, si se trata de empresa de ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, si la empresa es de ámbito autonómico.

c) Depósito de almacenamiento y armero o caja fuerte, de las características y con el sistema de seguridad, en su caso, que determine el Ministerio del Interior.

4. Transporte y distribución de objetos valiosos o peligrosos y de explosivos.

4.1 Objetos valiosos o peligrosos.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a), 1.º

B) Segunda fase.

a) Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes de seguridad.

b) Seis vehículos blindados, si la empresa es de ámbito estatal y dos, si la empresa es de ámbito autonómico. Los vehículos tendrán las características que determine el Ministerio del Interior, estarán dotados de permiso de circulación, tarjeta de industrial y certificado acreditativo de la superación de la inspección técnica, todo ello a nombre de la empresa solicitante.

c) Local destinado exclusivamente a la guarda de los vehículos blindados fuera de las horas de servicio.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.

b) Una garantía de 240.404,84 euros, si la empresa es de ámbito estatal, y de 48.080,97 euros, más 12.020,24 euros por provincia, si es de ámbito autonómico.

c) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características que determine el Ministerio del Interior.

d) Disponer de un servicio de telecomunicación de voz entre los locales de la empresa, tanto el principal como los de las sucursales o delegaciones, y los vehículos que realicen el transporte.

4.2 Explosivos.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

a) Una plantilla compuesta por, al menos, dos vigilantes de explosivos por cada vehículo para el transporte de explosivos de que disponga la empresa y un jefe de seguridad cuando el número de vigilantes exceda de quince en total.

b) Disponer para el transporte de explosivos, al menos, de dos vehículos blindados con capacidad de carga superior a 1.000 kg cada uno, con las características que determina el Reglamento Nacional del Transporte de Mercancías Peligrosas por Carretera (TPC, tipo 2), y con las medidas de seguridad que se establezcan, debiendo aportar los documentos que para su acreditación determine el Ministerio del Interior.

c) Local para la guarda de los vehículos durante las horas en que permanecieren inmovilizados.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,42 euros por siniestro y año.

b) Una garantía de 120.202,42 euros, si la empresa es de ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, si es de ámbito autonómico.

c) Tener instalado armero o caja fuerte de las características que determine el Ministerio del Interior.

d) Disponer de un servicio de telecomunicación de voz entre los locales de la empresa, tanto el principal como los de las sucursales o delegaciones, y los vehículos que realicen el transporte.

5. Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a), 1.º

B) Segunda fase.

a) Relación de personal disponible en la que constará necesariamente el ingeniero técnico y los instaladores.

b) Una zona o área restringida que, con medios físicos, electrónicos o informáticos, garantice la custodia de la información que manejaren y de la que serán responsables.

C) Tercera fase.

a) Tener constituida una garantía de 120.202,42 euros, para el ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, para el ámbito autonómico.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros por siniestro y año.

6. Explotación de centrales de alarma.

A) Fase inicial

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

a) Elementos, equipos o sistemas capacitados para la recepción y verificación de las señales de alarma y su transmisión a las Fuerzas y Cuerpos de Seguridad.

b) Locales cuyos requisitos y características del sistema de seguridad determine el Ministerio del Interior.

c) Un sistema de alimentación ininterrumpida de energía que garantice durante veinticuatro horas, al menos, el funcionamiento de la central en el caso de corte del suministro de fluido eléctrico.

C) Tercera fase.

a) Tener constituida una garantía de 120.202,42 euros.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros.

7. Planificación y asesoramiento de actividades de seguridad.

A) Segunda fase.

a) Relación del personal disponible en la que constará necesariamente personal facultativo con la competencia suficiente para responsabilizarse de los proyectos, en los casos en que su actividad tenga por objeto el diseño de proyectos de instalaciones y sistemas de seguridad.

b) Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

c) Un área o zona restringida que, con medios físicos, electrónicos o informáticos, garantice la custodia de la información que manejare la empresa y de la que será responsable.

d) Cuando el asesoramiento o la planificación tengan por objeto alguna de las actividades a que se refieren los párrafos a), b), c) y d) del artículo 5 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, disponer, en la plantilla, de personal que acredite, mediante la justificación del desempeño de puestos o funciones de seguridad pública o privada, al menos, durante cinco años, conocimientos y experiencia sobre organización y realización de actividades de seguridad.

B) Tercera fase.

a) Tener constituida una garantía por importe de 60.101,21 euros.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros por siniestro y año.

8. Requisitos de las empresas que tengan su domicilio en Ceuta y Melilla.

Las empresas de seguridad con domicilio social en Ceuta y en Melilla, que pretendan desarrollar su actividad únicamente en el ámbito de una de dichas ciudades, deberán cumplir los mismos requisitos establecidos en el presente anexo.

II. Requisitos de las empresas de ámbito autonómico.

1. Las cantidades determinantes de los mínimos de garantía y de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada, especificadas en el apartado I de este anexo, como requisitos "De inscripción y autorización inicial", relativos a las empresas de ámbito autonómico, sean cuales fueren las actividades que realicen o servicios que presten, quedarán reducidas al 75 por ciento o al 50 por ciento, según que la población de derecho de las correspondientes comunidades autónomas sea inferior a 2.000.000 de habitantes y superior a 1.250.000, o inferior a 1.250.000 habitantes.

2. Las cantidades determinantes de los mínimos de garantía, especificadas en el apartado I de este anexo, relativas a las empresa de seguridad de ámbito autonómico, cualesquiera que fueren las actividades que realicen o servicios que presten, y cualquiera que fuere la población de derecho de las correspondientes comunidades autónomas, quedarán reducidas al 50 por ciento cuando se trate de empresas que, en el momento de la inscripción en el Registro, tengan una plantilla de menos de 50 trabajadores, y asimismo cuando, posteriormente, durante dos años consecutivos, no superen los 601.012,10 euros de facturación anual.

La reducción establecida en este apartado 2 no será acumulable a la relativa al mínimo de garantía, comprendida en lo dispuesto en el apartado anterior.

3. En los supuestos contemplados en los apartados 1 y 2 precedentes, no se computarán las cantidades por provincia, especificadas en el apartado I de este anexo, en cuanto a garantía, respecto a las provincias que tengan menos de 250.000 habitantes de población de derecho.

4. Respecto a las empresas de seguridad de ámbito autonómico, dedicadas exclusivamente a instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, los requisitos establecidos en el apartado I.5 de este anexo, se aplicarán con las modificaciones que se especifican a continuación:

a) No necesitarán tener un ingeniero técnico en la plantilla a tiempo total, cuando ésta integre menos de cinco puestos de instaladores, si bien, alternativamente, habrán de tenerlo a tiempo parcial, o deberán contar, de forma permanente, mediante contrato mercantil, con los servicios de un ingeniero técnico que supervise y garantice técnicamente la instalación y el mantenimiento de aparatos, dispositivos y sistemas. En todo caso, el ingeniero técnico habrá de estar específicamente cualificado par el ejercicio de su misión.

b) La garantía mínima a constituir será de 6.101,21 euros.

Sin embargo, será de 12.020,24 euros, cuando se trate de empresas no constituidas en forma de sociedad.

c) El contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada cubrirá una garantía mínima de 60.101,21 euros.

5. Las modificaciones de plantillas de las empresas autonómicas a que se refiere el presente apartado, que den lugar a su inclusión o exclusión del supuesto regulado en el apartado 2 anterior, producirán el cambio de los requisitos de inscripción y autorización de dichas empresas y determinarán la instrucción de los correspondientes expedientes de modificaciones de inscripción.

6. Cuando las empresas pretendan actuar en comunidades autónomas limítrofes, sin abarcar la totalidad del territorio nacional, deberán inscribirse en el Registro General de Empresas de Seguridad, pero podrán hacerlo con aplicación de los criterios cuantitativos, establecidos en este anexo, conjuntamente a los ámbitos territoriales autonómicos correspondientes, como si se tratara de un territorio autonómico único.

INFORMACIÓN RELACIONADA:
- Las referencias hechas al Ministerio de Justicia e Interior, a la Secretaría de Estado de Interior, y a los Gobiernos Civiles, se entenderán efectuadas al Ministerio del Interior, a la Secretaría de Estado de Seguridad, y a las Delegaciones del Gobierno, respectivamente, conforme establece la disposición adicional cuarta del Real Decreto 1123/2001, de 19 de octubre. Ref. BOE-A-2001-21874.

§ 21

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 166, de 12 de julio de 2002
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2002-13758

[. . .]

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e

implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.

[...]

§ 22

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional

Ministerio de Defensa
«BOE» núm. 68, de 19 de marzo de 2004
Última modificación: sin modificaciones
Referencia: BOE-A-2004-5051

La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional.

Entre los elementos más característicos de esta nueva situación figuran el desarrollo alcanzado por las tecnologías de la información, la facilidad y flexibilidad de su transmisión en diversos soportes, la generalización casi universal de su uso y la accesibilidad global a las diversas herramientas y redes. Todos estos rasgos facilitan el intercambio ágil y flexible de información en las sociedades modernas.

Al mismo tiempo, la elaboración, conservación y utilización de determinada información por parte de la Administración es necesaria para garantizar su funcionamiento eficaz al servicio de los intereses nacionales.

En consecuencia, la Administración debe dotarse de los medios adecuados para la protección y control del acceso a dicha información, y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios.

Razones de eficacia, economía y coherencia administrativa recomiendan el establecimiento de medidas para regular y coordinar la adquisición del sofisticado material que se precisa, la homologación de su capacidad y compatibilidad, sus procedimientos de empleo y la formación técnica del personal de la Administración especialista en este campo. Asimismo, ha de elaborarse y mantenerse actualizada la normativa relativa a la protección de la información clasificada y velar por su cumplimiento, para evitar el acceso a ésta de individuos, grupos y Estados no autorizados.

El concepto de seguridad de los sistemas de información no sólo abarca la protección de la confidencialidad de ésta; en la mayoría de los casos es necesario también que los sistemas permitan el acceso de los usuarios autorizados, funcionen de manera íntegra y garanticen que la información que manejan mantiene su integridad. En consecuencia, la seguridad de los sistemas de información debe garantizar la confidencialidad, la disponibilidad y la integridad de la información que manejan y la disponibilidad y la integridad de los propios sistemas.

Se hace necesaria la participación de un organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de productos y sistemas. A partir de

esa garantía, los responsables de los sistemas de información podrán implementar los productos y sistemas que satisfagan los requisitos de seguridad de la información.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Este real decreto se dicta en virtud de lo dispuesto en la disposición final primera de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

En su virtud, a propuesta del Ministro de Defensa, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 12 de marzo de 2004,

DISPONGO:

Artículo 1. *Del Director del Centro Criptológico Nacional.*

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica.

Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo.

Artículo 2. *Del ámbito de actuación y funciones del Centro Criptológico Nacional.*

1. El ámbito de actuación del Centro Criptológico Nacional comprende:

a) La seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.

b) La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada.

2. Dentro de dicho ámbito de actuación, el Centro Criptológico Nacional realizará las siguientes funciones:

a) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Para el desarrollo de estas funciones, el CCN podrá establecer la coordinación oportuna con las comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las tecnologías de la información y de las comunicaciones.

3. El Centro Criptológico Nacional queda adscrito al Centro Nacional de Inteligencia y comparte con éste medios, procedimientos, normativa y recursos, y se regirá por la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. El personal del CCN estará integrado orgánica y funcionalmente en el Centro Nacional de Inteligencia, por lo que le serán de aplicación todas las disposiciones relativas al personal de éste, contempladas en la Ley 11/2002, de 6 de mayo, y en la normativa de desarrollo, particularmente su régimen estatutario.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Facultades de desarrollo.*

Se faculta al Ministro de Defensa para dictar cuantas disposiciones sean necesarias para la aplicación y el desarrollo de lo establecido en este real decreto.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 23

Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial]

Ministerio de Defensa
«BOE» núm. 252, de 17 de octubre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-10520

[. . .]

TÍTULO II

Estructura operativa de las Fuerzas Armadas

[. . .]

CAPÍTULO II

Organización del Estado Mayor de la Defensa

Sección 1.ª Funciones y estructura organizativa del Estado Mayor de la Defensa

Artículo 9. *El Estado Mayor de la Defensa.*

1. El Estado Mayor de la Defensa es el órgano que posibilita el cumplimiento de sus funciones al Jefe de Estado Mayor de la Defensa. Se organizará de forma que permita la definición y el desarrollo de la estrategia militar, el planeamiento militar, el planeamiento, seguimiento y conducción de las operaciones militares y el ejercicio del resto de sus competencias.

2. Entre otras funciones, al Estado Mayor de la Defensa le corresponderá:

a) El desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones, así como la dirección de la ejecución y el control del cumplimiento de estas políticas.

b) La planificación, dirección y, en su caso, ejecución, en su ámbito, de las actuaciones en materia de cartografía.

c) La dirección y coordinación de la sanidad operativa.

3. El Estado Mayor de la Defensa se estructura en un Cuartel General y los siguientes órganos:

a) El Mando de Operaciones.
b) El Centro de Inteligencia de las Fuerzas Armadas.
c) El Mando Conjunto de Ciberdefensa.
d) El Centro Superior de Estudios de la Defensa Nacional.

4. Además, en el Estado Mayor de la Defensa se integran:

a) Las organizaciones operativas permanentes.
b) Los órganos nacionales militares relacionados con organizaciones internacionales o multinacionales.

[. . .]

Sección 3.ª Los órganos de la estructura del Estado Mayor de la Defensa

[. . .]

Artículo 15. *El Mando Conjunto de Ciberdefensa.*

El Mando Conjunto de Ciberdefensa será responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

[. . .]

§ 24

Orden DEF/166/2015, de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas. [Inclusión parcial]

Ministerio de Defensa
«BOE» núm. 35, de 10 de febrero de 2015
Última modificación: 18 de septiembre de 2015
Referencia: BOE-A-2015-1232

La Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, reguló las bases de la organización militar conforme a los principios constitucionales y respondiendo a los principios de jerarquía, disciplina, unidad y eficacia y con criterios que posibilitasen la acción conjunta en las Fuerzas Armadas (FAS), que se constituyen como una entidad única e integradora de las distintas formas de acción de sus componentes y que posibilita el empleo óptimo de sus capacidades, sin que aquéllos vean mermada su especificidad. Su artículo 11 establece que las FAS se organizan en dos estructuras, la orgánica y la operativa.

La estructura orgánica, compuesta por el Ejército de Tierra, la Armada y el Ejército del Aire, prepara la fuerza y posibilita la generación de la estructura operativa. Ésta, establecida para el desarrollo de la acción conjunta y combinada, emplea la fuerza en las misiones que se le asignen.

Recientemente se ha publicado el Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas, en adelante el Real Decreto, con dos objetivos principales: establecer la organización de las FAS simplificando sus estructuras y adoptando una terminología común y eliminar la dispersión normativa mediante la derogación de los reales decretos que hasta esa fecha regían esta materia.

Así, el Real Decreto incide en conceptos básicos para el funcionamiento de este modelo de FAS, como son los de eficacia operativa y servicio unificado.

En consecuencia, el Real Decreto subordina las organizaciones operativas permanentes al JEMAD, atribuyéndole la competencia para promulgar la doctrina militar nacional y establece un nuevo concepto de empleo de las Fuerzas Armadas, la Fuerza Conjunta. Además, se crea la Jefatura de Apoyo para la Acción Conjunta con el objetivo de concentrar y potenciar el apoyo a este tipo de acción.

Asimismo, el Real Decreto destaca las competencias que el JEMAD tiene de coordinar a los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire para asegurar la eficacia operativa de las FAS, de impartirles directrices para orientar la preparación de la Fuerza, de supervisar dicha preparación y de evaluar la disponibilidad operativa de las unidades de la Fuerza y le da otras nuevas en el ámbito de la organización de los Ejércitos, pudiendo proponer medidas encaminadas a su homogeneización para mejorar la eficacia operativa de las FAS o a la unificación de servicios no exclusivos de un ejército.

En cuanto a la estructura orgánica y como consecuencia de la reciente reorganización del Ministerio de Defensa, centralizando la logística de obtención y de la asunción por parte

del Estado Mayor de la Defensa (EMAD) de cometidos no exclusivos de alguno de los Ejércitos, éstos sufren modificaciones, tanto en la concreción de las competencias de sus Jefes de Estado Mayor, como en las competencias que asumen los elementos que los constituyen, el Cuartel General, la Fuerza y el Apoyo a la Fuerza, que sufren las modificaciones organizativas precisas para adecuarse a este nuevo reparto de competencias.

La disposición final segunda del Real Decreto 872/2014, de 10 de octubre, faculta al Ministro de Defensa para que adopte las medidas necesarias para su desarrollo y ejecución.

Así se llega a esta orden ministerial que tiene tres objetivos; el establecimiento de unas normas básicas de organización de las Fuerzas Armadas, el desarrollo de la organización básica de las Fuerzas Armadas establecida por el Real Decreto y la eliminación de la dispersión normativa mediante la derogación de las órdenes ministeriales que hasta la fecha rigen esta materia.

La orden ministerial incluye tres artículos con el fin de establecer unas normas básicas de organización de las FAS. El primero de ellos define el elemento organizativo básico de las FAS, el segundo establece el modo de crear, modificar y suprimir unidades y el tercero establece unas normas elementales de organización.

Partiendo de la orgánica actualmente existente y con arreglo a las competencias que para cada órgano define el Real Decreto, estas normas básicas sirven de marco común de referencia y evitan la reiteración en la definición de las misiones, funciones y cometidos de las unidades que tengan una misma denominación. Para ello, se establecen una serie de órganos comunes y sus funciones que determinan un esquema básico organizativo válido para cualquier unidad.

Para el desarrollo de la organización básica establecida en el Real Decreto se han tenido en cuenta los aspectos que se detallan en los párrafos siguientes.

No se regulan aquellos órganos ya establecidos en el Real Decreto ya que la mera repetición de lo dispuesto en el Real Decreto no aportaría una mejor comprensión del texto normativo y aumentaría en exceso su volumen.

Se definen exclusivamente la misión, las funciones y los cometidos principales de las unidades que se regulan, sin detallar actividades que puedan derivarse de aquellas. Tampoco se incluyen aquellas funciones asignadas en virtud de otra normativa legal o reglamentaria vigente o que tengan asumidas en virtud de convenio u otras formas de colaboración con entidades públicas o privadas.

No se incluye ninguna referencia a acciones o actividades concretas de los jefes de las diferentes unidades, ya que éstos tienen las competencias que las leyes y reglamentos les atribuyen, siendo responsables de que su unidad cumpla con la misión encomendada, no habiendo necesidad de detallar acciones y actividades que puedan derivarse de su condición de jefe. Tampoco se establecen cometidos que puedan corresponderles a los jefes/ comandantes de mandos operativos que les sean propios como consecuencia de la aplicación de la doctrina militar.

Se homogeneizan órganos y estructuras similares, tanto en la esquematización de su definición como en los tiempos verbales y en la terminología empleada. No se incluyen definiciones de vocabulario propio de la terminología operativa y que cae dentro del ámbito de la doctrina militar.

No se establecen los empleos militares concretos de determinados puestos ya que es competencia del Subsecretario de Defensa y de los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire el establecimiento de las plantillas orgánicas y de las relaciones de puestos militares.

Finalmente, la disposición de esta orden ministerial se ha realizado con arreglo a la estructura del Real Decreto y se ha establecido un mecanismo de transición a la nueva organización.

En esta orden ministerial, con arreglo a lo que establece el artículo 21.3 de la Ley 39/2007, de 19 de noviembre, de la carrera militar, cuando se utilice una denominación básica de un empleo militar se entenderá que comprende las específicas de cada ejército.

En su virtud, dispongo:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Finalidad.*

La finalidad de esta orden ministerial es desarrollar la organización básica de las Fuerzas Armadas (FAS) establecida en el Real Decreto 872/2014, de 10 de octubre.

Artículo 2. *Elemento organizativo básico de las Fuerzas Armadas.*

1. En las Fuerzas Armadas el elemento organizativo básico será la «unidad» que comprende el conjunto de personal, material y medios de apoyo organizados y preparados para la ejecución de las misiones y los cometidos que se le asignen, vinculados orgánicamente por una jefatura común. Su entidad o dimensión y su naturaleza será consecuencia del tipo de misión a desarrollar. Esta definición incluye tanto a las unidades militares y buques de la Fuerza como a cualquier centro u otro tipo de organismo encuadrado en las Fuerzas Armadas.

2. Las unidades podrán ser agrupadas entre sí para formar otras de entidad superior.

3. En función de su entidad y de la misión a desarrollar las unidades podrán recibir las denominaciones que se deriven de la doctrina militar de las Fuerzas Armadas y de su tradición. No obstante, no podrán utilizarse denominaciones que legalmente estén reservadas para nombrar órganos superiores y directivos de la Administración General del Estado.

4. Para el desempeño de sus funciones, las unidades desplegarán o se ubicarán en bases, acuartelamientos, arsenales, aeródromos militares o establecimientos.

5. Las unidades de las Fuerzas Armadas se crearán, modificarán y suprimirán conforme a lo establecido en esta orden ministerial, salvo que una disposición de rango superior establezca lo contrario.

Artículo 3. *Creación, modificación y supresión de unidades.*

1. La creación de cualquier unidad exigirá el cumplimiento de los siguientes requisitos:

a) Definición de su misión y de sus funciones y cometidos.
b) Determinación de su dependencia jerárquica y estructura interna.
c) Dotación de los créditos necesarios para su puesta en marcha y funcionamiento.
d) Modificación de las relaciones de puestos militares y, en su caso, de la relación de puestos de trabajo que sean precisas.

2. Salvo en la Fuerza, no podrán crearse nuevas unidades que supongan duplicación de otras ya existentes si al mismo tiempo no se suprimen o restringen debidamente las funciones o cometidos de éstas.

3. Las unidades cuyo jefe deba ser nombrado por el Ministro de Defensa y las unidades pertenecientes a la Fuerza cuyo mando corresponda al empleo de coronel se crearán y suprimirán por orden del Ministro de Defensa.

También se crearán y suprimirán por orden del Ministro de Defensa aquellas unidades cuyo mando corresponda al empleo de coronel que, no perteneciendo a la Fuerza, no se encuadren dentro de un cuartel general o una jefatura, en los términos establecidos en el artículo 4, apartados 4 y 6.

4. Las unidades de nivel inmediatamente inferior a las que hace referencia el apartado anterior se crearán y suprimirán por resolución del Jefe de Estado Mayor de la Defensa o del Jefe de Estado Mayor de su respectivo ejército, con el informe favorable del Subsecretario de Defensa en el ámbito de sus competencias.

5. Las reestructuraciones organizativas dentro de las unidades citadas en los apartados anteriores y la creación de unidades de nivel inferior podrán realizarse mediante la modificación de las correspondientes relaciones de puestos militares y, en su caso, de las relaciones de puestos de trabajo, en los términos legalmente previstos.

Artículo 4. *Normas básicas de organización.*

1. La estructura de las unidades respetará de forma general el modelo formado por: Mando, órgano de apoyo al Mando y unidades subordinadas.

2. El Mando, Jefe o Comandante de una unidad, será el responsable del funcionamiento de la misma y tendrá las competencias que legal y reglamentariamente se le atribuyan.

3. Los órganos de apoyo al Mando son unidades que le asisten en el ejercicio de sus competencias y prestan apoyo a aquellas otras unidades que el Mando determine.

4. Un cuartel general es una estructura organizativa de medios humanos y materiales encuadrados en unidades que prestan su apoyo al Mando. Por lo general, estará constituido por un estado mayor y otras unidades que asisten al Mando.

5. Un estado mayor es responsable de proporcionar al Mando los elementos de juicio necesarios para fundamentar sus decisiones, traducir éstas en órdenes y velar por su cumplimiento. Un estado mayor realizará la planificación, coordinación y control de las actividades que se deriven de la misión, funciones y cometidos asignados a la unidad de la que forma parte. Un estado mayor nunca llevará a cabo acciones de mando ni de gestión ni ejecutivas.

6. El Mando de una unidad junto con sus órganos de apoyo personal e inmediato forman la Jefatura o Comandancia de la unidad.

7. En las unidades que cuenten con una Asesoría Jurídica, ésta será el órgano consultivo y asesor en materia jurídica del Mando de dicha unidad y de aquellas otras que éste determine y dependerá funcionalmente de la Asesoría Jurídica General de la Defensa a través de la Asesoría Jurídica del Cuartel General de su ejército.

8. En las unidades en las que exista una Intervención Delegada, ésta ejercerá el control interno de la gestión económico-financiera, la Notaría Militar y el asesoramiento económico-fiscal de las unidades que se le asignen y dependerá orgánica y funcionalmente de la Intervención General de la Defensa.

9. Las unidades subordinadas son aquellas que ejecutan las acciones necesarias para llevar a cabo la misión encomendada a la unidad de la que forman parte. También podrán existir otras unidades subordinadas que tengan funciones de apoyo a la unidad de la que forman parte.

[. . .]

Artículo 6. *El Estado Mayor Conjunto de la Defensa.*

1. El Estado Mayor Conjunto de la Defensa (EMACON) se articula en:

a) La Jefatura.
b) La Secretaría General del Estado Mayor Conjunto de la Defensa (SEGEMACON).
c) La División de Planes (DIVPLA)
d) La División de Estrategia (DIVESTRA).

2. La Jefatura estará formado por el Jefe del Estado Mayor Conjunto de la Defensa (JEMACON) y sus órganos de apoyo personal.

3. La SEGEMACON será el órgano responsable de auxiliar directamente al JEMACON en la dirección del EMACON, así como del apoyo técnico-administrativo a los órganos del Cuartel General del EMAD. Le corresponde, también, el asesoramiento y apoyo en los asuntos que, siendo responsabilidad del EMACON, no son específicos de las divisiones que lo componen.

4. La DIVPLA será responsable de elaborar y coordinar el planeamiento de Fuerza, de desarrollar los cometidos relacionados con el proceso de obtención de recursos materiales en los que JEMAD sea competente y de orientar los procesos de transformación de las capacidades operativas de las FAS. Asimismo, será responsable de elaborar y coordinar la postura de las FAS ante las organizaciones internacionales de seguridad y defensa (OISD) en el ámbito logístico.

5. La DIVESTRA será responsable de elaborar y desarrollar la estrategia militar y el concepto de empleo de las FAS. Asimismo, será responsable de elaborar y coordinar la

postura de las FAS ante las OISD en las que el JEMAD tenga responsabilidades, de planear, coordinar y controlar las actividades derivadas de las relaciones militares de carácter bilateral y multilateral que competen a éste y de confeccionar las opciones de respuesta militar para apoyar al JEMAD en el planeamiento y conducción estratégica de las operaciones.

[. . .]

Artículo 8. *Los órganos de apoyo al mando, de asistencia y de servicios generales.*

1. Los órganos de apoyo al mando, de asistencia y de servicios generales son los siguientes:

a) La Secretaría Permanente del Consejo de Jefes de Estado Mayor.
b) La Secretaría del JEMAD.
c) La Jefatura de Asuntos Económicos (JAE).
d) La Jefatura de Recursos Humanos (JRRHH).
e) La Jefatura de Seguridad y Servicios (JESES).

2. La Secretaría Permanente del Consejo de Jefes de Estado Mayor actuará como órgano administrativo de dicho consejo y de aquellos otros consejos y reuniones que el JEMAD le encomiende.

3. La Secretaría del JEMAD será responsable del planeamiento, coordinación y ejecución de las actividades públicas y protocolarias del JEMAD y de estudiar, asesorar y tramitar los asuntos que le afecten como representante institucional de las FAS. También será responsable de las actividades relacionadas con los medios de comunicación social en el ámbito del EMAD, así como de coordinar los actos militares que sean responsabilidad del JEMAD.

4. La JAE será responsable de la dirección, gestión, administración y control de los recursos financieros bajo la dependencia del JEMAD, a quien asesorará en todo lo concerniente a estas materias y a asuntos presupuestarios, así como de la contratación y contabilidad. Le corresponderá, también, la elaboración técnica del anteproyecto de presupuesto y la centralización de toda la información tanto sobre la previsión y ejecución de los programas como del presupuesto. Dependerá funcionalmente de la Dirección General de Asuntos Económicos.

5. La JRRHH será responsable del planeamiento y gestión del recurso de personal militar y civil dependiente del JEMAD, del apoyo administrativo y logístico a dicho personal. También prestará asesoramiento en el ámbito de la enseñanza competencia del JEMAD. Será la representante ante las OISD en los aspectos de recursos humanos del ámbito de responsabilidad del EMAD.

6. La JESESE será responsable del mantenimiento de las instalaciones, apoyando en materia de vida y funcionamiento al Cuartel General del EMAD y a aquellas unidades dependientes del JEMAD que se determinen y a sus componentes. Organizará y dirigirá la seguridad que precise el personal destinado en el Cuartel General del EMAD y de sus dependencias.

Artículo 9. *El Mando de Operaciones.*

1. Además de las responsabilidades establecidas para el Mando de Operaciones (MOPS) en el artículo 13 del Real Decreto 872/2014, de 10 de octubre, corresponden al Comandante del Mando de Operaciones (CMOPS), en los términos que establezca el JEMAD en la doctrina militar, los siguientes cometidos principales:

a) Planear y conducir las operaciones necesarias para cumplir las misiones de las Fuerzas Armadas de carácter nacional que se determinen.
b) Planear y conducir las operaciones multinacionales cuando España asuma su liderazgo.
c) Ejercer el mando de las fuerzas puestas bajo su autoridad de acuerdo con lo establecido en los planes en vigor.

d) Planear y conducir los ejercicios conjuntos necesarios para asegurar la eficacia operativa de las fuerzas de los Ejércitos asignadas y para la evaluación de los planes operativos.

e) Planear la participación de fuerzas españolas en operaciones y ejercicios conjunto-combinados que no sean de responsabilidad nacional, efectuar el seguimiento de su actuación y empleo por la cadena operativa multinacional y dirigir su sostenimiento.

f) Gestionar y coordinar los medios necesarios para el despliegue, sostenimiento, repliegue y apoyo de las fuerzas asignadas, controlando tanto la estimación de las necesidades como la gestión de los recursos financieros puestos a disposición de las FAS para la financiación de operaciones.

g) Planear y dirigir las evaluaciones sobre la disponibilidad operativa de las unidades de la Fuerza mediante la valoración de su grado de alistamiento.

2. El MOPS se articula en:

a) La Comandancia.
b) La 2.ª Comandancia.
c) El Estado Mayor (EMMOPS).
d) El Mando Conjunto de Operaciones Especiales (MCOE).

3. La Comandancia está formado por el CMOPS y sus órganos de apoyo personal.

4. La 2.ª Comandancia estará al mando del 2.º Comandante del MOPS, quien podrá asumir, en su caso, la dirección de todas las actividades del MOPS.

5. El EMMOPS será el órgano al que corresponde la planificación, coordinación y control general de todas las actividades del MOPS, siendo su Jefe el 2.º Comandante.

6. El MCOE será responsable de realizar el planeamiento, conducción y seguimiento de las operaciones especiales que se determinen, así como de facilitar la integración e interoperabilidad de las capacidades de operaciones especiales, y de planificar y conducir los ejercicios conjuntos necesarios para asegurar la eficacia operativa de las unidades de operaciones especiales que le sean asignadas. Así mismo, asesorará al JEMAD y al CMOPS en todo lo referente a operaciones especiales.

Artículo 10. *El Centro de Inteligencia de las Fuerzas Armadas.*

El Centro de Inteligencia de las Fuerzas Armadas (CIFAS), con arreglo a lo que establece la disposición adicional primera del Real Decreto 872/2014, de 10 de octubre, tendrá los cometidos específicos y la estructura que se establezcan en su orden ministerial clasificada en la categoría de «secreto».

[. . .]

Artículo 12. *El Centro Superior de Estudios de la Defensa Nacional.*

1. El Centro Superior de Estudios de la Defensa Nacional (CESEDEN) se articula en:

a) La Escuela Superior de las Fuerzas Armadas (ESFAS).
b) El Instituto Español de Estudios Estratégicos (IEEE).
c) El Centro Conjunto de Desarrollo de Conceptos (CCDC).
d) La Comisión Española de Historia Militar (CEHISMI).

2. La ESFAS impartirá cursos de altos estudios de la defensa nacional, incluidos los de actualización para el desempeño de los cometidos de oficial general y para la obtención del Diploma de Estado Mayor de las Fuerzas Armadas, así como los estudios conducentes a la obtención de títulos de posgrado y específicos militares que se determinen. Además, colaborará con otros organismos competentes para investigar y analizar los resultados sobre aquellos aspectos relacionados con las doctrinas para la acción conjunta y combinada.

3. El IEEE desarrollará actividades que investiguen temas relacionados con la defensa y la seguridad y promuevan el interés de la sociedad en estos temas para contribuir al fomento y difusión de la cultura de defensa.

4. El CCDC dirigirá y coordinará el estudio de nuevos conceptos operativos que sirvan de apoyo para la potenciación de las capacidades militares, manteniendo con los

organismos homólogos de los países aliados y las organizaciones internacionales, así como con la Dirección General de Armamento y Material, las relaciones necesarias para la colaboración y el intercambio de información. Así mismo, promoverá y coordinará el estudio y desarrollo de la doctrina conjunta y combinada, manteniendo las relaciones que sean precisas con los órganos de las FAS y las organizaciones internacionales responsables en esta materia, a través del análisis de las lecciones identificadas y las carencias doctrinales.

5. La CEHISMI es un órgano colegiado que promoverá, impulsará y desarrollará actividades relacionadas con la historia militar que afecten a más de un ejército o a la Guardia Civil y ejercerá la representación nacional en los organismos internacionales de historia militar en los casos en que así se acuerde.

6. En el desempeño de sus actividades el CESEDEN dependerá funcionalmente de la Subsecretaría de Defensa y de la Secretaría General de Política de Defensa, en el ámbito de sus respectivas competencias.

Artículo 13. *El Mando de Vigilancia y Seguridad Marítima.*

1. El Mando de Vigilancia y Seguridad Marítima (MVSM) es el órgano de la estructura operativa de las Fuerzas Armadas responsable del planeamiento, conducción y seguimiento de las operaciones de vigilancia y seguridad de los espacios marítimos de soberanía, responsabilidad e interés nacional.

2. El Almirante de la Flota (ALFLOT) será el Comandante del Mando de Vigilancia y Seguridad Marítima.

3. Corresponderá al Comandante del MVSM planear y conducir las operaciones de vigilancia y seguridad de los espacios marítimos nacionales que el JEMAD determine y ejercer el mando de las fuerzas puestas bajo su autoridad de acuerdo con lo establecido en los planes en vigor, conforme con la doctrina militar. También le corresponderá planear y conducir las operaciones multinacionales de vigilancia y seguridad de espacios marítimos cuando España asuma su liderazgo, cuando lo determine el JEMAD.

4. El Comandante del MVSM mantendrá, en el ejercicio de sus responsabilidades, relaciones de coordinación con las autoridades y organismos militares y civiles, nacionales e internacionales, relacionadas con las operaciones que el JEMAD determine.

5. Como organización operativa permanente, el MVSM está directamente subordinado al JEMAD y, en la ejecución de las operaciones que se le asignen, estará bajo el control operacional del CMOPS, con arreglo a lo que establece el artículo 6.2 del Real Decreto 872/2014, de 10 de octubre.

Artículo 14. *El Mando de Defensa y Operaciones Aéreas.*

1. El Mando de Defensa y Operaciones Aéreas (MDOA) es el órgano de la estructura operativa de las Fuerzas Armadas responsable del planeamiento, conducción y seguimiento de las operaciones de vigilancia, seguridad, control y policía aérea en los espacios aéreos de soberanía, responsabilidad e interés nacional.

2. El General Jefe del Mando Aéreo de Combate del Ejército del Aire (GJMACOM) será el Comandante del Mando de Defensa y Operaciones Aéreas.

3. Corresponderá al Comandante del MDOA planear y conducir las operaciones de vigilancia, control, seguridad y policía aérea en y desde los espacios aéreos de soberanía, responsabilidad e interés nacional, y ejercer el mando de las fuerzas puestas bajo su autoridad de acuerdo con lo establecido en los planes en vigor, conforme con la doctrina militar. También le corresponderá planear y conducir las operaciones multinacionales de vigilancia, control, seguridad y policía aérea en y desde el espacio aéreo cuando España asuma su liderazgo, cuando lo determine el JEMAD.

4. El Comandante del MDOA mantendrá, en el ejercicio de sus responsabilidades, relaciones de coordinación con las autoridades y organismos militares y civiles, nacionales e internacionales, relacionadas con las operaciones que el JEMAD determine.

5. Como organización operativa permanente, el MDOA está directamente subordinado al JEMAD y, en la ejecución de las operaciones que se le asignen, estará bajo el control operacional del CMOPS, con arreglo a lo que establece el artículo 6.2 del Real Decreto 872/2014, de 10 de octubre.

Artículo 15. *La Unidad Militar de Emergencias.*

1. La Unidad Militar de Emergencias (UME) depende orgánica y operativamente del JEMAD y se constituye de forma permanente como un mando conjunto de la estructura operativa de las Fuerzas Armadas.

2. La UME dependerá funcionalmente de la Secretaría de Estado de Defensa, de la Subsecretaría de Defensa y de la Secretaría General de Política de Defensa, en los ámbitos de sus respectivas competencias.

3. Al Jefe de la UME, que será un oficial general del Ejército de Tierra, le corresponde su mando, dirección, organización, preparación y empleo operativo, conforme a lo dispuesto en la doctrina militar y en su protocolo específico de intervención.

4. Para auxiliar al Jefe de la UME en sus cometidos, podrá nombrarse a un Segundo Jefe.

5. La UME está constituida por un Cuartel General, en el que contará con una Asesoría Jurídica y existirá una Intervención Delegada, y las siguientes unidades subordinadas:

a) Un Batallón de Transmisiones.
b) Cinco Batallones de Intervención.
c) Un Regimiento de Apoyo e Intervención en Emergencias.

6. Para el desempeño de las misiones de la UME, el JEMAD podrá requerir de los Ejércitos las unidades o los apoyos que sean necesarios cuando la naturaleza de la emergencia así lo requiera y con arreglo a la doctrina militar.

7. Los Ejércitos apoyarán al JEMAD en la gestión de los recursos materiales de que disponga la UME y en sus actividades de apoyo logístico que posibiliten su vida y funcionamiento y su operatividad.

8. Con carácter general, el coste de los apoyos que se presten a las unidades de la UME se compensarán a los Ejércitos con arreglo a la normativa en vigor.

Artículo 16. *Representaciones militares nacionales y otros órganos dependientes del JEMAD.*

1. Conforme con lo establecido en el artículo 20 del Real Decreto 872/2014, de 10 de octubre, dependen del JEMAD las representaciones militares ante las OISD, el personal destinado en puestos militares de la OTAN, de la UE, de los Cuarteles Generales Multinacionales, de otros centros u organismos cuyos puestos pertenezcan al ámbito de competencias del JEMAD, así como los elementos nacionales, los elementos nacionales de apoyo y los contingentes nacionales integrados en organizaciones internacionales y multinacionales en las que España participe.

2. Todo el personal reseñado tendrá como uno de sus cometidos principales asegurar la debida coordinación y unidad de acción de los esfuerzos de las FAS conducentes a garantizar los intereses españoles en dichas organizaciones como parte de la Acción Exterior del Estado.

3. Las citadas representaciones militares tendrán además las siguientes funciones generales:

a) Ejecutar labores de enlace y de representación, así como servir de canal oficial de comunicación entre el JEMAD y las organizaciones internacionales ante los que esté acreditado.

b) Contribuir, en estrecha colaboración con los correspondientes órganos del EMAD, a la preparación y elaboración de la postura de las FAS ante las organizaciones internacionales.

CAPÍTULO III

Los Cuarteles Generales del Ejército de Tierra, de la Armada y del Ejército del Aire

Artículo 17. *Desarrollo de la organización de los cuarteles generales.*

Con arreglo a lo establecido en el título III, capítulo II del Real Decreto 872/2014, de 10 de octubre, el Cuartel General de cada ejército está constituido por:

a) El Estado Mayor.
b) El Gabinete del Jefe de Estado Mayor.
c) Los órganos de asistencia y servicios generales del Cuartel General.
d) La Asesoría Jurídica.
e) La Intervención Delegada.

Artículo 18. *El Estado Mayor.*

1. El Estado Mayor se articula en:

a) La Jefatura.
b) La Secretaría General del Estado Mayor.
c) La División de Planes.
d) La División de Operaciones.
e) La División de Logística.

2. La Jefatura estará formada por el Segundo Jefe del Estado Mayor y sus órganos de apoyo personal.

3. La Secretaría General del Estado Mayor será el principal órgano de apoyo al Segundo Jefe del Estado Mayor de cada ejército y será responsable de todos aquellos asuntos del Estado Mayor que no sean competencia específica de alguna de sus divisiones.

4. La División de Planes será responsable de la organización y planeamiento global de su ejército a medio y largo plazo, de actualizar los planes y de la definición inicial, seguimiento y coordinación de los programas de ellos derivados.

5. La División de Operaciones será responsable del planeamiento, coordinación y control general de los objetivos a alcanzar en cuanto a la preparación de las unidades de su ejército y del seguimiento de sus actividades para, en su caso, su puesta a disposición de la estructura operativa de las FAS.

6. La División de Logística será responsable del planeamiento, coordinación y control general de los objetivos a alcanzar en cuanto al apoyo logístico.

Artículo 19. *Los órganos de asistencia y servicios generales del Cuartel General.*

1. Los órganos de asistencia y servicios generales del Cuartel General son los siguientes:

a) Los órganos de asistencia técnica.
b) Los órganos de historia y cultura militar.
c) Los órganos de servicios generales.

2. Los órganos de asistencia técnica serán responsables de todas aquellas actividades relacionadas con los Sistemas de Información y Telecomunicaciones, cartografía, publicaciones, sociología, estadística, investigación operativa e información de su respectivo ejército.

En el Ejército de Tierra será la Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica, en la Armada será la Jefatura de Servicios Generales, Asistencia Técnica y Sistemas de la Información y Telecomunicaciones y en el Ejército del Aire, la Jefatura de Servicios Técnicos y de Sistemas de Información y Telecomunicaciones.

Dependerán funcionalmente de los órganos directivos del departamento competentes por razón de materia. En el caso concreto de los Sistemas de Información y

Telecomunicaciones existirá, además, una dependencia funcional del EMAD y de la Secretaría de Estado de la Defensa, en el ámbito de sus respectivas competencias.

3. Los órganos de historia y cultura militar serán responsables de la protección, conservación, catalogación, investigación y divulgación del patrimonio histórico, cultural, documental y bibliográfico de su respectivo ejército.

En el Ejército de Tierra asumirá estos cometidos el Instituto de Historia y Cultura Militar, en la Armada, el Órgano de Historia y Cultura Naval y en el Ejército del Aire, el Servicio Histórico y Cultural del Ejército del Aire.

Estos órganos de historia y cultura militar dependerán funcionalmente de los órganos superiores y directivos del departamento competentes por razón de materia.

4. Los órganos de servicios generales serán responsables de proporcionar seguridad y apoyo al Cuartel General y a las unidades que determine su Jefe de Estado Mayor, así como de facilitar su vida y funcionamiento, y atender al mantenimiento de las instalaciones.

En el Ejército de Tierra el órgano de servicios generales será el Regimiento de Infantería «Inmemorial del Rey» n.º 1, en la Armada, la Jefatura de Servicios Generales, Asistencia Técnica y Sistemas de la Información y Telecomunicaciones y, en el Ejército del Aire, la Agrupación del Cuartel General del Ejército del Aire.

CAPÍTULO IV

La Fuerza

Artículo 20. *Fuerza del Ejército de Tierra.*

1. La estructura de la Fuerza del Ejército de Tierra será flexible y adaptable, permitiendo dar una respuesta rápida y eficaz al empleo de las fuerzas terrestres en escenarios complejos e inciertos. La característica fundamental que definirá esta estructura será la polivalencia de sus unidades de nivel brigada, que se materializará en una Fuerza con un conjunto de capacidades que puedan dar respuesta a las exigencias operativas en todo el espectro del conflicto.

2. La Fuerza del Ejército de Tierra está constituida por los siguientes órganos, dependientes directamente del Jefe de Estado Mayor del Ejército de Tierra:

a) Cuartel General Terrestre de Alta Disponibilidad.
b) Fuerza Terrestre.
c) Fuerza Logística Operativa.
d) Mando de Canarias.

3. El Cuartel General Terrestre de Alta Disponibilidad se rige por su norma específica de creación.

4. La Fuerza Terrestre se articula en:

a) Cuartel General.

b) División «San Marcial» y División «Castillejos», que son un conjunto de unidades que tienen por cometido principal prepararse para constituir, de forma rápida y eficaz, estructuras operativas de acuerdo con la doctrina militar.

La División «San Marcial» se articula en:

1.º Cuartel General.
2.º Brigada «Guzmán el Bueno» X.
3.º Brigada «Extremadura» XI.
4.º Brigada «Guadarrama» XII.
5.º Brigada «Aragón» I.

La División «Castillejos» se articula en:

1.º Cuartel General.
2.º Brigada «Rey Alfonso XIII» II de La Legión.
3.º Brigada «Almogávares» VI de Paracaidistas.
4.º Brigada «Galicia» VII.

c) Comandancias Generales de Ceuta, Melilla y Baleares, que son un conjunto de unidades, ubicadas en la Ciudad de Ceuta, en la Ciudad de Melilla y en la Comunidad Autónoma de las Illes Balears respectivamente, que tienen por cometido principal prepararse para constituir estructuras operativas de acuerdo con la doctrina militar.

d) Fuerzas Aeromóviles del Ejército de Tierra, que son un conjunto de unidades aeromóviles o con capacidad aeromóvil, puestas bajo un mando único y organizadas, equipadas y adiestradas para ser empleadas en apoyo de las unidades que se determinen o en el marco de otras organizaciones operativas, de acuerdo con la doctrina militar.

e) Mando de Operaciones Especiales, que es un conjunto de unidades de operaciones especiales y de unidades de apoyo a las mismas, puestas bajo un mando único y organizadas, equipadas y adiestradas para realizar operaciones especiales en el marco de una organización operativa, de acuerdo con la doctrina militar.

f) Mando de Artillería de Campaña, que es un conjunto de unidades de artillería de campaña y de costa puestas bajo un mando único y organizadas, equipadas y adiestradas para ser empleadas en refuerzo de la artillería de campaña de las unidades que se determinen o en el marco de una organización operativa y en el control y defensa de costas, de acuerdo con la doctrina militar.

g) Mando de Artillería Antiaérea, que es un conjunto de unidades, básicamente de artillería antiaérea, puestas bajo un mando único y organizadas, equipadas y adiestradas para su empleo en apoyo a la artillería antiaérea de las unidades que se determinen o en el marco de una organización operativa y para proporcionar defensa antiaérea de otras unidades, puntos y zonas del territorio nacional, de acuerdo con la doctrina militar.

h) Mando de Ingenieros, que es un conjunto de unidades de ingenieros puestas bajo un mando único y organizadas, equipadas y adiestradas para su empleo en apoyo y refuerzo de las unidades que se determinen y en el marco de cualquier otra organización operativa, de acuerdo con la doctrina militar.

i) Mando de Transmisiones, que es un conjunto de unidades de transmisiones puestas bajo un mando único y organizadas, equipadas y adiestradas para su empleo en refuerzo a las unidades de transmisiones de las unidades que se determinen y para proporcionar apoyo CIS/EW en el marco de una organización operativa, de acuerdo con la doctrina militar.

j) Aquellas otras unidades del Ejército de Tierra que se determinen.

5. La Fuerza Logística Operativa se articula en:

a) Cuartel General.

b) Brigada Logística, que es un conjunto de unidades de apoyo logístico al combate puestas bajo un mando único, adiestradas y equipadas para ser empleadas en apoyo de las unidades que se determinen o en el marco de una organización operativa de superior nivel, de acuerdo con la doctrina militar. También prestan apoyo logístico a las unidades, complementando la estructura permanente de Apoyo a la Fuerza.

c) Brigada de Sanidad, que es un conjunto de unidades sanitarias puestas bajo un mando único, adiestradas y equipadas para prestar el apoyo sanitario para las operaciones, de acuerdo con la doctrina militar. También prestan apoyo sanitario a las unidades, complementando la estructura permanente de Apoyo a la Fuerza.

6. El Mando de Canarias se articula en el Cuartel General, la Brigada «Canarias» XVI y otras unidades del Ejército de Tierra ubicadas en el archipiélago canario.

Artículo 21. *Fuerza de la Armada.*

1. La Fuerza de la Armada está constituida por la Flota, dependiente directamente del Jefe de Estado Mayor de la Armada.

2. La Flota se articula en:

a) Cuartel General.

b) La Fuerza de Acción Naval, constituida por un Estado Mayor y un conjunto de unidades navales preparadas para constituir, de forma rápida y eficaz, las organizaciones operativas que puedan ser necesarias para la realización de operaciones navales, de acuerdo con la doctrina militar. En su seno se encuadra orgánicamente el Cuartel General Marítimo de Alta Disponibilidad que se rige por su norma específica.

c) La Fuerza de Acción Marítima, constituida por un Estado Mayor y un conjunto de unidades preparadas para efectuar, de acuerdo con la doctrina militar, en los espacios de interés nacional, misiones principalmente relacionadas con la seguridad marítima y con la libertad de acción, mediante la presencia y vigilancia en los espacios marítimos de interés y la contribución al conjunto de actividades que llevan a cabo las administraciones públicas con responsabilidad en el ámbito marítimo.

d) La Fuerza de Infantería de Marina, constituida por un Estado Mayor y un conjunto de unidades preparadas principalmente para constituir, de forma rápida y eficaz, las organizaciones operativas para la realización de operaciones militares iniciadas en la mar, incluyendo acción en tierra y la Guerra Naval Especial, así como dar protección y seguridad física de las personas y unidades de la Armada, de acuerdo con la doctrina militar.

e) Flotilla de Submarinos, que es la unidad que agrupa a los submarinos de la Armada para dirigir su preparación que les permita integrarse en unidades operativas, de acuerdo con la doctrina militar.

f) Flotilla de Aeronaves, que es la unidad que agrupa a las aeronaves de la Armada para dirigir su preparación que les permita constituirse en unidades aéreas embarcadas e integrarse en unidades operativas, de acuerdo con la doctrina militar.

g) Centro de Evaluación y Certificación para el Combate, para la evaluación y certificación de unidades para el combate y el apoyo al adiestramiento.

h) Centro de Doctrina de la Flota, para el análisis y desarrollo de la doctrina y procedimientos de empleo de unidades.

Artículo 22. *Fuerza del Ejército del Aire.*

1. La Fuerza del Ejército del Aire está constituida por los siguientes órganos, dependientes directamente del Jefe de Estado Mayor del Ejército del Aire:

a) Mando Aéreo de Combate.
b) Mando Aéreo General.
c) Mando Aéreo de Canarias.

2. El Mando Aéreo de Combate se articula en:

a) El Cuartel General, en el que está integrado el Centro de Operaciones Aéreas, cuyo cometido principal será prepararse para ser utilizado como órgano desde el que se ejerce el mando y control de las operaciones aéreas que se determinen, de acuerdo con la doctrina militar.

b) La Jefatura del Sistema de Mando y Control, que será responsable de dirigir, coordinar y evaluar las funciones del Sistema de Mando y Control del Ejército del Aire, que posibilitan la vigilancia y control del espacio aéreo de soberanía, responsabilidad e interés nacional así como la conducción de las operaciones aéreas, de acuerdo con la doctrina militar.

c) La Jefatura de Movilidad Aérea, que será responsable de dirigir y coordinar la utilización de los medios de transporte aéreo, reabastecimiento en vuelo, aeroevacuaciones médicas y de apoyo al despliegue del Ejército del Aire, siendo responsable de la coordinación de los medios nacionales que gestione el Mando Europeo de Transporte Aéreo (EATC), todo ello de acuerdo con la doctrina militar.

d) La Jefatura de Operaciones Aéreas Especiales y Recuperación de Personal, que será responsable de preparar, dirigir, coordinar y evaluar los medios humanos y materiales necesarios para llevar a cabo operaciones aéreas especiales y de recuperación de personal, de acuerdo con la doctrina militar. Incluye el Servicio de Búsqueda y Salvamento.

e) Las unidades del Ejército del Aire que se determinen.

3. El Mando Aéreo General contará con un Cuartel General y las unidades del Ejército del Aire que se determinen.

4. El Mando Aéreo de Canarias contará con un Cuartel General y las unidades del Ejército del Aire ubicadas en el archipiélago canario que se determinen.

CAPÍTULO V

El Apoyo a la Fuerza

Artículo 23. *Apoyo a la Fuerza en el ámbito de los recursos humanos.*

1. El Apoyo a la Fuerza en el ámbito de los recursos humanos será realizado por órganos competentes en las siguientes materias:

a) Personal, que será responsable de la dirección, gestión, administración y control del personal en materia de situaciones, ascensos, destinos, recompensas, documentación, evaluación, clasificación, orientación de carrera y cuantos asuntos condicionan la carrera militar, conforme a la normativa vigente. También será responsable de las actuaciones que puedan corresponder a su ejército en materia de reclutamiento y generación adicional de recursos humanos y de gestión del personal de los cuerpos comunes de las FAS, del personal civil y del personal reservista asignado a su respectivo ejército.

b) Asistencia al personal, que será responsable de la dirección, gestión, administración y control en materias de acción social y apoyo al personal y a sus familias, así como de las prestaciones sociales conforme a la normativa vigente. También será responsable de la dirección global en el ámbito de su ejército en materia de calidad de vida y podrá ser responsable en materia de promoción educativa y reintegración al mundo laboral.

c) Enseñanza, que será responsable de la dirección, inspección, coordinación así como de la evaluación, en materia de enseñanza militar de formación y de perfeccionamiento del personal militar. También podrá ser responsable en materia de investigación y de los medios y procedimientos de simulación.

d) Sanidad, que será responsable de la dirección, gestión, administración y control en materia de sanidad en sus aspectos preventivo, asistencial y pericial, y del asesoramiento en materia de apoyo sanitario logístico-operativo. También será responsable en materia de abastecimiento y mantenimiento de los recursos sanitarios, conforme a los procedimientos que establezca su ejército.

2. El Apoyo a la Fuerza en el ámbito de los recursos humanos del Ejército de Tierra será realizado por los siguientes órganos:

a) El Mando de Personal, que cuenta con una Jefatura y se articula en:

1.º La Dirección de Personal, que será responsable en materia de personal.

2.º La Dirección de Asistencia al Personal, que será responsable en materia de asistencia al personal.

3.º La Dirección de Sanidad, que será responsable en materia de sanidad.

b) El Mando de Adiestramiento y Doctrina, que cuenta con una Jefatura y se articula en:

1.º La Dirección de Investigación, Doctrina, Orgánica y Materiales, que será responsable de la dirección, inspección, coordinación e investigación en materias relacionadas con la evolución y experimentación teórica del combate, doctrina, normativa de empleo de las unidades, estructura y plantilla orgánica de las unidades del Ejército de Tierra, formulación de los requerimientos operativos del armamento, material y equipo, experimentación de materiales y del proceso de lecciones aprendidas.

2.º La Dirección de Enseñanza, Instrucción, Adiestramiento y Evaluación, que será responsable de la dirección, inspección, coordinación e investigación así como de la evaluación, en materia de enseñanza militar de formación y de perfeccionamiento del personal militar y de los medios y procedimientos de instrucción, adiestramiento y evaluación operativa del personal y de las unidades, así como de los medios y metodologías que sirvan de apoyo a la enseñanza, instrucción, adiestramiento y evaluación. También será responsable del desarrollo de las misiones derivadas de la legislación vigente en materia de educación físico-militar y de conducción y seguridad vial.

3. El Apoyo a la Fuerza en el ámbito de los recursos humanos en la Armada será realizado por la Jefatura de Personal, que cuenta con una Jefatura y se articula en:

a) La Dirección de Personal, que será responsable en materia de personal.
b) La Dirección de Asistencia al Personal, que será responsable en materia de asistencia al personal.
c) La Dirección de Enseñanza Naval, que será responsable en materia de enseñanza.
d) La Dirección de Sanidad, que será responsable en materia de sanidad.

4. El Apoyo a la Fuerza en el ámbito de los recursos humanos en el Ejército del Aire será realizado por el Mando de Personal, que cuenta con una Jefatura y se articula en:

a) La Dirección de Personal, que será responsable en materia de personal y de asistencia al personal.
b) La Dirección de Enseñanza, que será responsable en materia de enseñanza.
c) La Dirección de Sanidad, que será responsable en materia de sanidad.

Artículo 24. *Apoyo a la Fuerza en el ámbito de los recursos materiales.*

1. El Apoyo a la Fuerza en el ámbito de los recursos materiales será realizado por órganos competentes en las siguientes materias:

a) Adquisiciones, que será responsable de la dirección, gestión, administración y control en materia de adquisición de recursos materiales que no sean obtenidos de forma centralizada por otro organismo.
b) Abastecimiento y Transportes, que será responsable de la integración del apoyo logístico en lo relativo a dirección, gestión, administración, control y análisis en las materias de abastecimiento, excluida la adquisición, y de transporte.
c) Sostenimiento, que será responsable de la integración del apoyo logístico en lo relativo a dirección, gestión, administración, control y análisis en la materia de sostenimiento.
d) Infraestructura, que será responsable de la ejecución en materia de construcciones y obras, del mantenimiento y ordenación de las instalaciones, así como de los aspectos relacionados con la protección medioambiental.

2. El Apoyo a la Fuerza en el ámbito de los recursos materiales del Ejército de Tierra será realizado por los siguientes órganos:

a) El Mando de Apoyo Logístico, que cuenta con una Jefatura y se articula en:

1.º La Dirección de Adquisiciones, que será responsable en materia de adquisiciones.
2.º La Dirección de Integración de Funciones Logísticas, que será responsable en las materias de abastecimiento, excluida la adquisición, de sostenimiento y de transporte.

b) La Inspección General del Ejército de Tierra, que cuenta con una Jefatura y se articula en:

1.º La Dirección de Acuartelamiento, que será responsable de la programación, gestión, administración y control de las actividades, apoyos y recursos relacionados con la vida y funcionamiento de las unidades que no tengan carácter de preparación o logístico, de la seguridad de las bases, acuartelamientos y establecimientos y de su inventario. También será responsable de la prevención de riesgos laborales en aquellos aspectos contemplados en la normativa correspondiente, del desarrollo de la normativa sobre régimen interior en las bases, acuartelamientos y establecimientos y de los cometidos relativos a propiedades y a zonas e instalaciones de interés para la Defensa Nacional dentro del marco de sus capacidades.
2.º La Dirección de Infraestructura, que será responsable de la ejecución en materia de construcciones y obras, del mantenimiento y ordenación de las instalaciones, así como de los aspectos relacionados con la protección medioambiental.

3. El Apoyo a la Fuerza en el ámbito de los recursos materiales en la Armada será realizado por la Jefatura de Apoyo Logístico, que cuenta con una Jefatura y se articula en:

a) La Dirección de Ingeniería y Construcciones navales, que será responsable en materia de apoyo técnico de ingeniería para el sostenimiento de las unidades y sistemas de armas durante su ciclo de vida.

b) La Dirección de Abastecimiento y Transportes, que será responsable en las materias de abastecimiento, incluida la adquisición, y de transporte.

c) La Dirección de Sostenimiento, que será responsable en materia de sostenimiento de los recursos materiales.

d) La Dirección de Infraestructura, que será responsable en materia de infraestructura y de las actividades relacionadas con la administración y control de los recursos de infraestructura.

4. El Apoyo a la Fuerza en el ámbito de los recursos materiales del Ejército del Aire será realizado por el Mando de Apoyo Logístico, que cuenta con una Jefatura y se articula en:

a) La Dirección de Adquisiciones, que será responsable en materia de adquisiciones.

b) La Dirección de Sostenimiento y Apoyo Logístico Operativo, que será responsable en las materias de abastecimiento, excluida la adquisición, de sostenimiento y de transporte; así como de prestar apoyo logístico operativo a las unidades.

c) La Dirección de Ingeniería e Infraestructuras, que será responsable de las actividades relacionadas con la ingeniería aeronáutica aplicada y en materia de infraestructura.

Artículo 25. *Apoyo a la Fuerza en el ámbito de los recursos financieros.*

El Apoyo a la Fuerza en el ámbito de los recursos financieros en cada ejército será realizado por la Dirección de Asuntos Económicos, responsable de la dirección, gestión, administración y control de los recursos financieros puestos a disposición de su ejército y de la contratación y contabilidad. Le corresponderá también la elaboración técnica del anteproyecto de presupuesto y la centralización de toda la información tanto sobre la previsión y ejecución de los programas como del presupuesto. Asimismo, le corresponderá la administración de los recursos financieros no asignados expresamente a ningún otro órgano.

Artículo 26. *Dependencia funcional.*

Los órganos del Apoyo a la Fuerza de los Ejércitos enumerados en los artículos de este capítulo V dependerán funcionalmente de los órganos superiores y directivos del departamento competentes por razón de materia.

CAPÍTULO VI

El Consejo de Jefes de Estado Mayor

Artículo 27. *Organización del Consejo de Jefes de Estado Mayor.*

1. El Consejo de Jefes de Estado Mayor es un órgano consultivo en el que el JEMAD podrá recabar asesoramiento militar y coordinar a los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire para orientar la preparación de la Fuerza y asegurar la eficacia operativa de las FAS.

2. El Consejo de Jefes de Estado Mayor tendrá las siguientes funciones:

a) Apoyar al JEMAD, a requerimiento de éste, para ejercer sus responsabilidades como asesor militar del Presidente del Gobierno y del Ministro de Defensa y como conductor estratégico de las operaciones.

b) Asesorar al JEMAD en las siguientes cuestiones:

1.º Para establecer normas para la acción conjunta y para definir la estrategia militar.

2.º En asuntos relacionados con las capacidades militares de las Fuerzas Armadas.

3.º En el desarrollo de las operaciones.

4.º En la coordinación de asuntos relacionados con el régimen del personal militar en operaciones, en organismos conjuntos y en organizaciones internacionales en el ámbito de las FAS.

5.º En el establecimiento y coordinación de medidas que persigan la máxima eficacia operativa de las FAS.

c) Servir de instrumento de coordinación del JEMAD para orientar la preparación de la Fuerza y asegurar la eficacia operativa de las FAS.

3. El Consejo de Jefes de Estado Mayor estará compuesto por el JEMAD, que lo presidirá siempre que no asista el Ministro de Defensa, y los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire. Actuará de secretario del consejo, con voz pero sin voto, el jefe de la Secretaría Permanente del Consejo de Jefes de Estado Mayor.

4. El JEMAD, previo conocimiento del Ministro de Defensa, convocará el Consejo, estableciendo el orden del día, y le informará de los resultados.

5. En las reuniones del Consejo podrán participar otras autoridades que eventualmente sean requeridas para ello.

Disposición adicional primera. *Apoyo a las unidades ubicadas en la Base de Retamares.*

La Unidad de Apoyo General (UAG) de Retamares será responsable del apoyo, en materia de vida y funcionamiento y mantenimiento de las instalaciones, a las unidades dependientes de JEMAD ubicadas en la Base de Retamares, así como a sus componentes. Organiza y dirige la seguridad que precisen las instalaciones y el personal destinado de dichas Unidades. Dependerá directamente del Jefe de la Base de Retamares, que será la autoridad más antigua de las unidades del EMAD ubicadas en dicha base.

Disposición adicional segunda. *Composición y funcionamiento de la Comisión Española de Historia Militar.*

La CEHISMI estará compuesta por un presidente, cinco vocales natos, hasta cinco vocales electivos y un secretario.

El presidente será el Director del CESEDEN. La Comisión podrá designar entre sus miembros uno o varios vicepresidentes. Corresponde al Ministro de Defensa el nombramiento y cese de los vocales y del secretario, en las siguientes condiciones:

a) Vocales natos, habrá un representante de la Subdirección General de Publicaciones y Patrimonio Cultural a propuesta de su Subdirector General, un representante del Instituto de Historia y Cultura Militar, un representante del Órgano de Historia y Cultura Naval y un representante del Servicio Histórico y Cultural del Ejército del Aire, los tres a propuesta de sus directores respectivos, y un oficial del Servicio de Estudios Históricos de la Guardia Civil a propuesta de su Subdirector de Personal.

b) Vocales electivos, a propuesta del Director del CESEDEN, serán civiles o militares de reconocida especialización y prestigio.

c) Secretario, a propuesta del Director del CESEDEN, será un oficial destinado en el CESEDEN de acreditada especialización en el ámbito de la historia militar.

A las reuniones de la Comisión, el presidente podrá convocar a cuantas personas estime conveniente. Los convocados asistirán a la reunión con voz pero sin voto.

Como órgano de trabajo permanente y específico existirá una secretaría, constituida por el secretario de la Comisión y por el personal necesario para el cumplimiento de sus funciones. Dicha secretaría será atendida por personal destinado en el CESEDEN.

Disposición adicional tercera. *Órganos colegiados.*

1. En lo no regulado por esta orden ministerial, el funcionamiento de los órganos colegiados que en la misma se citan se ajustará a lo previsto en el título II, capítulo II, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. La pertenencia o participación en las reuniones de estos órganos colegiados no supondrá la percepción de ningún tipo de retribución o indemnización que suponga incremento del gasto público.

Disposición adicional cuarta. *Del Comandante General de la Infantería de Marina.*

Con arreglo a lo que establece la disposición adicional segunda del Real Decreto 872/2014, de 10 de octubre, sobre la potestad de asesorar directamente al Jefe de Estado Mayor de la Armada, en aquellos asuntos referidos al Cuerpo de Infantería de Marina que no se relacionen de forma específica y directa con la preparación de la Fuerza, del Comandante General de la Infantería de Marina, éste le podrá asesorar en todo lo relacionado con las virtudes, valores y espíritu tradicional del Cuerpo de Infantería de Marina. Asimismo, podrá asesorarle, cuando éste lo juzgue necesario, en otros asuntos referidos al Cuerpo de Infantería de Marina, tales como la organización de unidades, la formación militar, la progresión profesional, la doctrina terrestre y los métodos de empleo y la evolución de la Infantería de Marina. En estos casos mantendrá informado al Almirante de la Flota.

Disposición adicional quinta. *Organización de las unidades establecidas en esta orden ministerial.*

1. Las unidades descritas en esta orden ministerial se organizarán en unidades subordinadas con arreglo a lo dispuesto en los artículos 3 y 4.

2. En el plazo máximo de tres meses desde la entrada en vigor de esta orden ministerial el EMAD y los Ejércitos remitirán a la Subsecretaría de Defensa la organización vigente en la fecha de dicha entrada en vigor hasta el nivel establecido en el artículo 3.3 inclusive, con indicación, para cada una de las unidades, de sus funciones y cometidos y de su dependencia orgánica y, en su caso, funcional. En las unidades de la Fuerza se indicará el tipo de unidad de que se trata en función del tipo de operaciones para las que se prepara. También se especificarán aquellas otras funciones que las unidades realicen, asignadas por legislación especial o que tengan asumidas en virtud de convenio u otras formas de colaboración con entidades públicas o privadas, con indicación de esta circunstancia.

3. En el plazo máximo de cuatro meses desde la entrada en vigor de esta orden ministerial el EMAD y los Ejércitos remitirán a la Subsecretaría de Defensa las propuestas de modificación de sus respectivas organizaciones adaptadas a lo establecido en esta orden ministerial, en los mismos términos dispuestos en el apartado anterior.

Disposición adicional sexta. *Unidades dependientes operativamente del Jefe de la UME.*

El Batallón de Helicópteros de Emergencias II del Ejército de Tierra y el 43.º Grupo de Fuerzas Aéreas del Ejército del Aire dependerán operativamente del Jefe de la UME, conforme a lo dispuesto en la doctrina militar y en su protocolo específico de intervención.

Ambos ejércitos asegurarán, respectivamente, la operatividad de estas unidades.

Disposición adicional séptima. *Relaciones de la Armada.*

La Armada mantendrá las relaciones con la Administración marítima española y otras agencias marítimas de acuerdo con lo establecido en los acuerdos y convenios de colaboración suscritos con cada una de ellas.

Disposición adicional octava. *Control de la navegación aérea.*

El control de la navegación aérea, tanto general como operativa, continuará sometido a lo establecido en el artículo 4 de la Ley 21/2003, de 7 de julio, de seguridad aérea.

Disposición adicional novena. *No incremento del gasto público.*

La aplicación de esta orden ministerial, incluida la modificación de las unidades existentes y la creación de aquellas que sean necesarias, se hará sin aumento de coste de funcionamiento de las FAS y no supondrá incremento del gasto público.

Disposición transitoria única. *Unidades existentes.*

Las unidades de los Cuarteles Generales, de la Fuerza y del Apoyo a la Fuerza actualmente existentes, no contempladas en esta orden ministerial, pasarán a depender de

las unidades ahora establecidas en función de las misiones, funciones y cometidos encomendados a éstas, con arreglo a lo que dispongan el JEMAD y los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire, y continuarán ejerciendo sus funciones y cometidos hasta que entren en vigor las disposiciones que complementen o apliquen esta orden ministerial, se produzcan las adaptaciones orgánicas necesarias y se transfieran dichas funciones y cometidos a las nuevas unidades.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas las siguientes disposiciones:

a) Orden Ministerial 228/2001, de 24 de octubre, por la que se desarrollan las funciones del Instituto Español de Estudios Estratégicos.

b) Orden DEF/3537/2003, de 10 de diciembre, por la que se desarrolla la estructura orgánica básica de los Ejércitos, modificada por la Orden DEF/3229/2005, de 10 de octubre, y la Orden DEF/1298/2009, de 14 de mayo.

c) Orden DEF/1076/2005, de 19 de abril, por la que se desarrolla la estructura del Estado Mayor de la Defensa.

d) Orden Ministerial 114/2006, de 18 de septiembre, por la que se establecen las líneas generales del proceso de transición a la nueva estructura de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire y se dictan normas para su desarrollo y ejecución.

e) Orden DEF/448/2007, de 27 de febrero, por la que se modifica el despliegue de la Fuerza del Ejército del Aire, que figura en el anexo III del Real Decreto 416/2006, de 11 de abril, por el que se establece la organización y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, así como de la Unidad Militar de Emergencias.

f) Orden DEF/1766/2007, de 13 de junio, por la que se desarrolla el encuadramiento, organización y funcionamiento de la Unidad Militar de Emergencias.

g) Orden DEF/3771/2008, de 10 de diciembre, por la que se modifica la estructura orgánica y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, que figura en el Real Decreto 416/2006, de 11 abril, por el que se establece la organización y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, así como de la Unidad Militar de Emergencias.

h) Orden Ministerial 5/2009, de 11 de febrero, de creación del Consejo de Jefes de Estado Mayor.

i) Orden Ministerial 86/2012, de 4 de diciembre, por la que se crean el Mando de Vigilancia y Seguridad Marítima y el Mando de Defensa y Operaciones Aéreas.

j) Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en ésta orden ministerial.

Disposición final primera. *Facultades de desarrollo.*

Sin perjuicio de lo ordenado en la disposición adicional quinta, se faculta al Jefe de Estado Mayor de la Defensa y a los Jefes de Estado Mayor del Ejército de Tierra, de la Armada y del Ejército del Aire a desarrollar esta orden ministerial, con arreglo a los términos establecidos en sus artículos 3 y 4.

Disposición final segunda. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el mismo día de su publicación en el «Boletín Oficial del Estado».

§ 25

Orden DEF/1887/2015, de 16 de septiembre, por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial]

Ministerio de Defensa
«BOE» núm. 224, de 18 de septiembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-10042

[. . .]

ORGANIZACIÓN DEL ESTADO MAYOR DE LA DEFENSA

Artículo 1. *Organización del Estado Mayor de la Defensa.*

1. El Estado Mayor de la Defensa se estructura de la siguiente forma:

a) El Cuartel General del Estado Mayor de la Defensa.
b) El Mando de Operaciones.
c) El Centro de Inteligencia de las Fuerzas Armadas.
d) El Mando Conjunto de Ciberdefensa.
e) El Centro Superior de Estudios de la Defensa Nacional.

2. El Cuartel General del Estado Mayor de la Defensa está integrado por:

a) El Estado Mayor Conjunto de la Defensa, que se articula en:

1.º La Jefatura.
2.º La Secretaría General del Estado Mayor Conjunto de la Defensa.
3.º La División de Planes.
4.º La División de Estrategia.

b) La Jefatura de Apoyo para la Acción Conjunta, que se articula en:

1.º La Jefatura de Sanidad Operativa.
2.º La Jefatura de Sistemas de Información y Telecomunicaciones de las Fuerzas Armadas.
3.º La Unidad de Verificación Española.
4.º La Célula Nacional C-IED.

c) La Secretaría Permanente del Consejo de Jefes de Estado Mayor.
d) La Secretaría del Jefe de Estado Mayor de la Defensa.
e) La Jefatura de Asuntos Económicos.
f) La Jefatura de Recursos Humanos.

g) La Jefatura de Seguridad y Servicios.
h) La Asesoría Jurídica.
i) La Intervención Delegada.

3. Las unidades citadas, encuadradas en el Cuartel General del Estado Mayor de la Defensa, cuyo jefe no deba ser nombrado por el Ministro de Defensa, tendrán el nivel orgánico que se determine, con arreglo a lo que se establezca en sus correspondientes relaciones de puestos militares.

4. Además, en el Estado Mayor de la Defensa se integran:

a) Las organizaciones operativas permanentes:

1.º El Mando de Vigilancia y Seguridad Marítima.
2.º El Mando de Defensa y Operaciones Aéreas.
3.º La Unidad Militar de Emergencias.

b) Los órganos nacionales militares relacionados con organizaciones internacionales o multinacionales.

5. Pertenece al Estado Mayor de la Defensa la Unidad de Apoyo General de Retamares.

[. . .]

Artículo 3. *El Mando Conjunto de Ciberdefensa.*

El Mando Conjunto de Ciberdefensa se articula en:

a) El Estado Mayor.
b) La Jefatura de Operaciones, responsable de la dirección y ejecución de las operaciones de Ciberdefensa.
c) La Jefatura de Administración y Servicios, responsable de prestar los apoyos necesarios para el funcionamiento del Mando y que tendrá el nivel orgánico que se determine, con arreglo a lo que se establezca en su correspondiente relación de puestos militares.

[. . .]

§ 26

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Jefatura del Estado
«BOE» núm. 166, de 12 de julio de 2002
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2002-13758

JUAN CARLOS I REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Lo que la Directiva 2000/31/CE denomina "sociedad de la información" viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.

Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Eso es lo que pretende esta Ley, que parte de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, ocupándose tan sólo de aquellos aspectos que, ya sea por su novedad o por las

peculiaridades que implica su ejercicio por vía electrónica, no están cubiertos por dicha regulación.

II

Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información", que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España. Por "establecimiento" se entiende el lugar desde el que se dirige y gestiona una actividad económica, definición esta que se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario. La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un "establecimiento permanente" situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.

El lugar de establecimiento del prestador de servicios es un elemento esencial en la Ley, porque de él depende el ámbito de aplicación no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE.

Por lo demás, sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podrá restringirse la prestación de servicios provenientes de dichos Estados cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concreta en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resulte aplicable a las mismas.

III

Se prevé la anotación del nombre o nombres de dominio de Internet que correspondan al prestador de servicios en el registro público en que, en su caso, dicho prestador conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que la vinculación entre el prestador, su establecimiento físico y su "establecimiento" o localización en la red, que proporciona su dirección de Internet, sea fácilmente accesible para los ciudadanos y la Administración pública.

La Ley establece, asimismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de

estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables.

Destaca, por otra parte, en la Ley, su afán por proteger los intereses de los destinatarios de servicios, de forma que éstos puedan gozar de garantías suficientes a la hora de contratar un servicio o bien por Internet. Con esta finalidad, la Ley impone a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato. Cuando la contratación se efectúe con consumidores, el prestador de servicios deberá, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

En lo que se refiere a las comunicaciones comerciales, la Ley establece que éstas deban identificarse como tales, y prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario haya prestado su consentimiento.

IV

Se favorece igualmente la celebración de contratos por vía electrónica, al afirmar la Ley, de acuerdo con el principio espiritualista que rige la perfección de los contratos en nuestro Derecho, la validez y eficacia del consentimiento prestado por vía electrónica, declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de "forma escrita" que figura en diversas leyes.

Se aprovecha la ocasión para fijar el momento y lugar de celebración de los contratos electrónicos, adoptando una solución única, también válida para otros tipos de contratos celebrados a distancia, que unifica el criterio dispar contenido hasta ahora en los Códigos Civil y de Comercio.

Las disposiciones contenidas en esta Ley sobre aspectos generales de la contratación electrónica, como las relativas a la validez y eficacia de los contratos electrónicos o al momento de prestación del consentimiento, serán de aplicación aun cuando ninguna de las partes tenga la condición de prestador o destinatario de servicios de la sociedad de la información.

La Ley promueve la elaboración de códigos de conducta sobre las materias reguladas en esta Ley, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector.

Por su sencillez, rapidez y comodidad para los usuarios, se potencia igualmente el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información. Se favorece, además, el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando, en su caso, las normas que, sobre la utilización de dichos medios, establezca la normativa específica sobre arbitraje.

De conformidad con lo dispuesto en las Directivas 2000/31/CE y 98/27/CE, se regula la acción de cesación que podrá ejercitarse para hacer cesar la realización de conductas contrarias a la presente Ley que vulneren los intereses de los consumidores y usuarios. Para el ejercicio de esta acción, deberá tenerse en cuenta, además de lo dispuesto en esta Ley, lo establecido en la Ley general de incorporación de la Directiva 98/27/CE.

La Ley prevé, asimismo, la posibilidad de que los ciudadanos y entidades se dirijan a diferentes Ministerios y órganos administrativos para obtener información práctica sobre distintos aspectos relacionados con las materias objeto de esta Ley, lo que requerirá el establecimiento de mecanismos que aseguren la máxima coordinación entre ellos y la homogeneidad y coherencia de la información suministrada a los usuarios.

Finalmente, se establece un régimen sancionador proporcionado pero eficaz, como indica la Directiva 2000/31/CE, para disuadir a los prestadores de servicios del incumplimiento de lo dispuesto en esta Ley.

Asimismo, se contempla en la Ley una serie de previsiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información proporcionada por medios electrónicos, y muy especialmente a la información suministrada por las Administraciones públicas, compromiso al que se refiere la resolución del Consejo de la Unión Europea de 25 de marzo de 2002, sobre accesibilidad de los sitios web públicos y de su contenido.

La presente disposición ha sido elaborada siguiendo un amplio proceso de consulta pública y ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio, y en el Real Decreto 1337/1999, de 31 de julio.

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto

Artículo 1. *Objeto.*

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.

CAPÍTULO II

Ámbito de aplicación

Artículo 2. *Prestadores de servicios establecidos en España.*

1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Artículo 3. *Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.

b) Emisión de publicidad por instituciones de inversión colectiva.

c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Artículo 4. *Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.*

A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2.

Los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos, además, a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables.

Artículo 5. *Servicios excluidos del ámbito de aplicación de la Ley.*

1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información:

a) Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.

b) Los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

2. Las disposiciones de la presente Ley, con la excepción de lo establecido en el artículo 7.1, serán aplicables a los servicios de la sociedad de la información relativos a juegos de

azar que impliquen apuestas de valor económico, sin perjuicio de lo establecido en su legislación específica estatal o autonómica.

TÍTULO II

Prestación de servicios de la sociedad de la información

CAPÍTULO I

Principio de libre prestación de servicios

Artículo 6. *No sujeción a autorización previa.*

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.

Artículo 7. *Principio de libre prestación de servicios.*

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

Artículo 8. *Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del

derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de identificar al responsable del servicio de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento. Tal requerimiento exigirá la previa autorización judicial de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización, los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación.

3. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

4. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

5. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

6. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.

CAPÍTULO II

Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información

Sección 1.ª Obligaciones

Artículo 9. *Constancia registral del nombre de dominio.*

(Sin contenido)

Artículo 10. *Información general.*

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

Artículo 12. *Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.*

(Derogado)

Artículo 12 bis. *Obligaciones de información sobre seguridad.*

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados

contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.

Sección 2.ª Régimen de responsabilidad

Artículo 13. *Responsabilidad de los prestadores de los servicios de la sociedad de la información.*

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. *Responsabilidad de los operadores de redes y proveedores de acceso.*

1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.

2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

Artículo 15. *Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.*

Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.

2.º Que se ha imposibilitado el acceso a ella, o 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Artículo 16. *Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.*

1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.

Artículo 17. *Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.*

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

CAPÍTULO III

Códigos de conducta

Artículo 18. *Códigos de conducta.*

1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta que afecten a los consumidores y usuarios estarán sujetos, además, al capítulo V de la Ley 3/1991, de 10 de enero, de competencia desleal.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.

Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.

3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.

TÍTULO III

Comunicaciones comerciales por vía electrónica

Artículo 19. *Régimen jurídico.*

1. Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo.

4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.

Artículo 21. *Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Artículo 22. *Derechos de los destinatarios de servicios.*

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

TÍTULO IV

Contratación por vía electrónica

Artículo 23. *Validez y eficacia de los contratos celebrados por vía electrónica.*

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

Artículo 24. *Prueba de los contratos celebrados por vía electrónica.*

1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

Artículo 25. *Intervención de terceros de confianza.*

1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

Artículo 26. *Ley aplicable.*

Para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español, debiendo tomarse en consideración para su aplicación lo establecido en los artículos 2 y 3 de esta Ley.

Artículo 27. *Obligaciones previas a la contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

d) La lengua o lenguas en que podrá formalizarse el contrato.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.

4. Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Artículo 28. *Información posterior a la celebración del contrato.*

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o

b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.

2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.

En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

Artículo 29. *Lugar de celebración del contrato.*

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

TÍTULO V

Solución judicial y extrajudicial de conflictos

CAPÍTULO I

Acción de cesación

Artículo 30. *Acción de cesación.*

1. Contra las conductas contrarias a la presente Ley que lesionen intereses colectivos o difusos de los consumidores podrá interponerse acción de cesación.

2. La acción de cesación se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la presente Ley y a prohibir su reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.

3. La acción de cesación se ejercerá conforme a las prescripciones de la Ley de Enjuiciamiento Civil para esta clase de acciones.

Artículo 31. *Legitimación activa.*

Están legitimados para interponer la acción de cesación:

a) Las personas físicas o jurídicas titulares de un derecho o interés legítimo, incluidas aquéllas que pudieran verse perjudicadas por infracciones de las disposiciones contenidas en los artículos 21 y 22, entre ellas, los proveedores de servicios de comunicaciones electrónicas que deseen proteger sus intereses comerciales legítimos o los intereses de sus clientes.

b) Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.

c) Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, o, en su caso, en la legislación autonómica en materia de defensa de los consumidores.

d) El Ministerio Fiscal.

e) El Instituto Nacional del Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.

f) Las entidades de otros Estados miembros de la Unión Europea constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el "Diario Oficial de las Comunidades Europeas".

Los Jueces y Tribunales aceptarán dicha lista como prueba de la capacidad de la entidad habilitada para ser parte, sin perjuicio de examinar si la finalidad de la misma y los intereses afectados legitiman el ejercicio de la acción.

CAPÍTULO II

Solución extrajudicial de conflictos

Artículo 32. *Solución extrajudicial de conflictos.*

1. El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de

los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos, en los términos que establezca su normativa específica.

TÍTULO VI

Información y control

Artículo 33. *Información a los destinatarios y prestadores de servicios.*

Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.

Artículo 34. *Comunicación de resoluciones relevantes.*

1. El Consejo General del Poder Judicial remitirá al Ministerio de Justicia, en la forma y con la periodicidad que se acuerde mediante Convenio entre ambos órganos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y los prestadores de servicios de la sociedad de la información.

2. Los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos a que se refiere el artículo 32.1 comunicarán al Ministerio de Justicia los laudos o decisiones que revistan importancia para la prestación de servicios de la sociedad de la información y el comercio electrónico de acuerdo con los criterios indicados en el apartado anterior.

3. En la comunicación de las resoluciones, laudos y decisiones a que se refiere este artículo, se tomarán las precauciones necesarias para salvaguardar el derecho a la intimidad y a la protección de los datos personales de las personas identificadas en ellos.

4. El Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso de cualquier interesado a la información recibida de conformidad con este artículo.

Artículo 35. *Supervisión y control.*

1. El Ministerio de Industria, Energía y Turismo controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. En todo caso, y no obstante lo dispuesto en el apartado anterior, cuando las conductas realizadas por los prestadores de servicios de la sociedad de la información

estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan.

Artículo 36. *Deber de colaboración.*

1. Los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología y a los demás órganos a que se refiere el artículo anterior toda la información y colaboración precisas para el ejercicio de sus funciones.

Igualmente, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

2. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, estatales o autonómicas, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VII

Infracciones y sanciones

Artículo 37. *Responsables.*

Los prestadores de servicios de la sociedad de la información están sujetos al régimen sancionador establecido en este título cuando la presente Ley les sea de aplicación.

Cuando las infracciones previstas en el artículo 38.3 i) y 38.4 g) se deban a la instalación de dispositivos de almacenamiento y recuperación de la información como consecuencia de la cesión por parte del prestador del servicio de la sociedad de la información de espacios propios para mostrar publicidad, será responsable de la infracción, además del prestador del servicio de la sociedad de la información, la red publicitaria o agente que gestione directamente con aquel la colocación de anuncios en dichos espacios en caso de no haber adoptado medidas para exigirle el cumplimiento de los deberes de información y la obtención del consentimiento del usuario.

Artículo 38. *Infracciones.*

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.

2. Son infracciones muy graves:

a) **(Sin contenido)**

b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

c) **(Derogado)**

d) **(Derogado)**

3. Son infracciones graves:

a) **(Derogado)**

b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.

c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

g) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley.

h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.

i) La reincidencia en la comisión de la infracción leve prevista en el apartado 4 g) cuando así se hubiera declarado por resolución firme dictada en los tres años inmediatamente anteriores a la apertura del procedimiento sancionador.

4. Son infracciones leves:

a) El incumplimiento de lo previsto en el art. 12 bis.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g) Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2.

h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave.

Artículo 39. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el "Boletín Oficial del Estado", o en el diario oficial de la Administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración pública o en la página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, por el número de usuarios o de contratos afectados, y la gravedad del ilícito.

3. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

Artículo 39 bis. *Moderación de sanciones.*

1. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 40.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:
a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el órgano competente no hubiese sancionado o apercibido con anterioridad al infractor como consecuencia de la comisión de infracciones previstas en esta Ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 40. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

a) La existencia de intencionalidad.
b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.
c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.
d) La naturaleza y cuantía de los perjuicios causados.
e) Los beneficios obtenidos por la infracción.
f) Volumen de facturación a que afecte la infracción cometida.
g) La adhesión a un código de conducta o a un sistema de autorregulación publicitaria aplicable respecto a la infracción cometida, que cumpla con lo dispuesto en el artículo 18 o en la disposición final octava y que haya sido informado favorablemente por el órgano u órganos competentes.

Artículo 41. *Medidas de carácter provisional.*

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las

Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. *Multa coercitiva.*

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Energía y Turismo, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses.

Artículo 44. *Concurrencia de infracciones y sanciones.*

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. *Prescripción.*

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Disposición adicional primera. *Significado de los términos empleados por esta Ley.*

A los efectos de la presente Ley, los términos definidos en el anexo tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Medicamentos y productos sanitarios.*

La prestación de servicios de la sociedad de la información relacionados con los medicamentos y los productos sanitarios se regirá por lo dispuesto en su legislación específica.

Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente que se prestará también por medios electrónicos, conforme al procedimiento establecido reglamentariamente.

Disposición adicional cuarta. *Modificación de los Códigos Civil y de Comercio.*

Uno. Se modifica el artículo 1.262 del Código Civil, que queda redactado de la siguiente manera:

> «El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.
>
> Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Dos. Se modifica el artículo 54 del Código de Comercio, que queda redactado de la siguiente manera:

«Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Disposición adicional quinta. *Accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.*

Uno. Las Administraciones públicas adoptarán las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005.

A partir del 31 de diciembre de 2008, las páginas de Internet de las Administraciones Públicas satisfarán, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

Las Administraciones Públicas exigirán que tanto las páginas de Internet cuyo diseño o mantenimiento financien total o parcialmente como las páginas de Internet de entidades y empresas que se encarguen de gestionar servicios públicos apliquen los criterios de accesibilidad antes mencionados. En particular, será obligatorio lo expresado en este apartado para las páginas de Internet y sus contenidos de los Centros públicos educativos, de formación y universitarios, así como, de los Centros privados que obtengan financiación pública.

Las páginas de Internet de las Administraciones Públicas deberán ofrecer al usuario información sobre su nivel de accesibilidad y facilitar un sistema de contacto para que puedan transmitir las dificultades de acceso al contenido de las páginas de Internet o formular cualquier queja, consulta o sugerencia de mejora.

Dos. Igualmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y "software", para facilitar el acceso de las personas con discapacidad o de edad avanzada a los contenidos digitales.

Tres. Las Administraciones Públicas promoverán medidas de sensibilización, educación y formación sobre accesibilidad con objeto de promover que los titulares de otras páginas de Internet incorporen progresivamente los criterios de accesibilidad.

Cuatro. Los incumplimientos de las obligaciones de accesibilidad establecidas en esta Disposición adicional estarán sometidos al régimen de infracciones y sanciones vigente en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

Cinco. Las páginas de Internet de las empresas que presten servicios al público en general de especial trascendencia económica, sometidas a la obligación establecida en el artículo 2 de la Ley 56/2007, de medidas de impulso de la sociedad de la información, deberán satisfacer a partir del 31 de diciembre de 2008, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente, esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad.

Seis. Las páginas de Internet que sirvan de soporte o canal a las redes sociales en línea, desarrolladas por entidades cuyo volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.101.121,04 euros, deberán satisfacer, a partir del 31 de diciembre de 2012, como mínimo, el nivel medio de los criterios de accesibilidad al contenido generalmente reconocidos. Excepcionalmente,

esta obligación no será aplicable cuando una funcionalidad o servicio no disponga de una solución tecnológica que permita su accesibilidad

Disposición adicional sexta. *Sistema de asignación de nombres de dominio bajo el ".es".*

Uno. Esta disposición regula, en cumplimiento de lo previsto en la disposición adicional decimosexta de la Ley 17/2001, de 7 de diciembre, de Marcas, los principios inspiradores del sistema de asignación de nombres de dominio bajo el código de país correspondiente a España ".es".

Dos. La entidad pública empresarial Red.es es la autoridad de asignación, a la que corresponde la gestión del registro de nombres de dominio de Internet bajo el ".es", de acuerdo con lo establecido en la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Tres. La asignación de nombres de dominio de Internet bajo el ".es" se realizará de conformidad con los criterios que se establecen en esta disposición, en el Plan Nacional de Nombres de Dominio de Internet, en las demás normas específicas que se dicten en su desarrollo por la autoridad de asignación y, en la medida en que sean compatibles con ellos, con las prácticas generalmente aplicadas y las recomendaciones emanadas de las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Los criterios de asignación de nombres de dominio bajo el ".es" deberán garantizar un equilibrio adecuado entre la confianza y seguridad jurídica precisas para el desarrollo del comercio electrónico y de otros servicios y actividades por vía electrónica, y la flexibilidad y agilidad requeridas para posibilitar la satisfacción de la demanda de asignación de nombres de dominio bajo el ".es", contribuyendo, de esta manera, al desarrollo de la sociedad de la información en España.

Podrán crearse espacios diferenciados bajo el ".es", que faciliten la identificación de los contenidos que alberguen en función de su titular o del tipo de actividad que realicen. Entre otros, podrán crearse indicativos relacionados con la educación, el entretenimiento y el adecuado desarrollo moral de la infancia y juventud. Estos nombres de dominio de tercer nivel se asignarán en los términos que se establezcan en el Plan Nacional de Nombres de Dominio de Internet.

Cuatro. Podrán solicitar la asignación de nombres de dominio bajo el ".es", en los términos que se prevean en el Plan Nacional de Nombres de Dominio de Internet, todas las personas o entidades, con o sin personalidad jurídica, que tengan intereses o mantengan vínculos con España, siempre que reúnan los demás requisitos exigibles para la obtención de un nombre de dominio.

Los nombres de dominio bajo el ".es" se asignarán al primer solicitante que tenga derecho a ello, sin que pueda otorgarse, con carácter general, un derecho preferente para la obtención o utilización de un nombre de dominio a los titulares de determinados derechos.

La asignación de un nombre de dominio confiere a su titular el derecho a su utilización, el cual estará condicionado al cumplimiento de los requisitos que en cada caso se establezcan, así como a su mantenimiento en el tiempo. La verificación por parte de la autoridad de asignación del incumplimiento de estos requisitos dará lugar a la cancelación del nombre de dominio, previa la tramitación del procedimiento que en cada caso se determine y que deberá garantizar la audiencia de los interesados.

Los beneficiarios de un nombre de dominio bajo el ".es" deberán respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres de dominio bajo el ".es".

La responsabilidad del uso correcto de un nombre de dominio de acuerdo con las leyes, así como del respeto a los derechos de propiedad intelectual o industrial, corresponde a la persona u organización para la que se haya registrado dicho nombre de dominio, en los términos previstos en esta Ley. La autoridad de asignación procederá a la cancelación de aquellos nombres de dominio cuyos titulares infrinjan esos derechos o condiciones, siempre que así se ordene en la correspondiente resolución judicial, sin perjuicio de lo que se prevea en aplicación del apartado ocho de esta disposición adicional.

Cinco. En el Plan Nacional de Nombres de Dominio de Internet se establecerán mecanismos apropiados para prevenir el registro abusivo o especulativo de nombres de

dominio, el aprovechamiento indebido de términos de significado genérico o topónimos y, en general, para prevenir los conflictos que se puedan derivar de la asignación de nombres de dominio.

Asimismo, el Plan incluirá las cautelas necesarias para minimizar el riesgo de error o confusión de los usuarios en cuanto a la titularidad de nombres de dominio.

A estos efectos, la entidad pública empresarial Red.es establecerá la necesaria coordinación con los registros públicos españoles. Sus titulares deberán facilitar el acceso y consulta a dichos registros públicos, que, en todo caso, tendrá carácter gratuito para la entidad.

Cinco bis. La autoridad de asignación suspenderá cautelarmente o cancelará, de acuerdo con el correspondiente requerimiento judicial previo, los nombres de dominio mediante los cuales se esté cometiendo un delito o falta tipificado en el Código Penal. Del mismo modo procederá la autoridad de asignación cuando por las Fuerzas y Cuerpos de Seguridad del Estado se le dirija requerimiento de suspensión cautelar dictado como diligencia de prevención dentro de las 24 horas siguientes al conocimiento de los hechos.

Asimismo, de acuerdo con lo dispuesto en los artículos 8, 11 y concordantes de esta Ley, la autoridad administrativa o judicial competente como medida para obtener la interrupción de la prestación de un servicio de la sociedad de la información o la retirada de un contenido, podrá requerir a la autoridad de asignación para que suspenda cautelarmente o cancele un nombre de dominio.

De la misma forma se procederá en los demás supuestos previstos legalmente.

En los supuestos previstos en los dos párrafos anteriores, sólo podrá ordenarse la suspensión cautelar o la cancelación de un nombre de dominio cuando el prestador de servicios o persona responsable no hubiera atendido el requerimiento dictado para el cese de la actividad ilícita.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá requerir la suspensión cautelar o la cancelación. En particular, cuando dichas medidas afecten a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrán ser decididas por los órganos jurisdiccionales competentes.

La suspensión consistirá en la imposibilidad de utilizar el nombre de dominio a los efectos del direccionamiento en Internet y la prohibición de modificar la titularidad y los datos registrales del mismo, si bien podrá añadir nuevos datos de contacto. El titular del nombre de dominio únicamente podrá renovar el mismo o modificar la modalidad de renovación. La suspensión cautelar se mantendrá hasta que sea levantada o bien, confirmada en una resolución definitiva que ordene la cancelación del nombre de dominio.

La cancelación tendrá los mismos efectos que la suspensión hasta la expiración del período de registro y si el tiempo restante es inferior a un año, por un año adicional, transcurrido el cual el nombre de dominio podrá volver a asignarse.

Seis. La asignación de nombres de dominio se llevará a cabo por medios telemáticos que garanticen la agilidad y fiabilidad de los procedimientos de registro.

La presentación de solicitudes y la práctica de notificaciones se realizarán por vía electrónica, salvo en los supuestos en que así esté previsto en los procedimientos de asignación y demás operaciones asociadas al registro de nombres de dominio.

Los agentes registradores, como intermediarios en los procedimientos relacionados con el registro de nombres de dominio, podrán prestar servicios auxiliares para la asignación y renovación de éstos, de acuerdo con los requisitos y condiciones que determine la autoridad de asignación, los cuales garantizarán, en todo caso, el respeto al principio de libre competencia entre dichos agentes.

Siete. El Plan Nacional de Nombres de Dominio de Internet se aprobará mediante Orden del Ministro de Ciencia y Tecnología, a propuesta de la entidad pública empresarial Red.es.

El Plan se completará con los procedimientos para la asignación y demás operaciones asociadas al registro de nombres de dominio y direcciones de Internet que establezca el Presidente de la entidad pública empresarial Red.es, de acuerdo con lo previsto en la

disposición adicional decimoctava de la Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social.

Ocho. En los términos que permitan las disposiciones aplicables, la autoridad de asignación podrá establecer un sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio, incluidos los relacionados con los derechos de propiedad industrial. Este sistema, que asegurará a las partes afectadas las garantías procesales adecuadas, se aplicará sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

Nueve. Con la finalidad de impulsar el desarrollo de la Administración electrónica, la entidad pública empresarial Red.es podrá prestar el servicio de notificaciones administrativas telemáticas y acreditar de forma fehaciente la fecha y hora de su recepción.

Disposición adicional séptima. *Fomento de la Sociedad de la Información.*

El Ministerio de Ciencia y Tecnología como Departamento de la Administración General del Estado responsable de la propuesta al Gobierno y de la ejecución de las políticas tendentes a promover el desarrollo en España de la Sociedad de la Información, la generación de valor añadido nacional y la consolidación de una industria nacional sólida y eficiente de productos, servicios y contenidos de la Sociedad de la Información, presentará al Gobierno para su aprobación y a las Cortes Generales un plan cuatrienal para el desarrollo de la Sociedad de la Información y de convergencia con Europa con objetivos mensurables, estructurado en torno a acciones concretas, con mecanismos de seguimiento efectivos, que aborde de forma equilibrada todos los frentes de actuación, contemplando diversos horizontes de maduración de las iniciativas y asegurando la cooperación y la coordinación del conjunto de las Administraciones públicas.

Este plan establecerá, asimismo, los objetivos, las acciones, los recursos y la periodificación del proceso de convergencia con los países de nuestro entorno comunitario en línea con las decisiones y recomendaciones de la Unión Europea.

En este sentido, el plan deberá:

Potenciar decididamente las iniciativas de formación y educación en las tecnologías de la información para extender su uso; especialmente, en el ámbito de la educación, la cultura, la gestión de las empresas, el comercio electrónico y la sanidad.

Profundizar en la implantación del gobierno y la administración electrónica incrementando el nivel de participación ciudadana y mejorando el grado de eficiencia de las Administraciones públicas.

Disposición adicional octava. *Colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas.*

1. Los registros de nombres de dominio establecidos en España estarán sujetos a lo establecido en el apartado Cinco bis de la disposición adicional sexta, respecto de los nombres de dominio que asignen.

2. Las entidades de registro de nombres de dominio establecidas en España estarán obligadas a facilitar los datos relativos a los titulares de los nombres de dominio que soliciten las autoridades públicas para el ejercicio de sus competencias de inspección, control y sanción cuando las infracciones administrativas que se persigan tengan relación directa con la actividad de una página de Internet identificada con los nombres de dominio que asignen.

Tales datos se facilitarán así mismo, cuando sean necesarios para la investigación y mitigación de incidentes de ciberseguridad en los que estén involucrados equipos relacionados con un nombre de dominio de los encomendados a su gestión. Dicha información será proporcionada al órgano, organismo o entidad que se determine legal o reglamentariamente.

En ambos supuestos, la solicitud deberá formularse mediante escrito motivado en el que se especificarán los datos requeridos y la necesidad y proporcionalidad de los datos solicitados para el fin que se persigue. Si los datos demandados son datos personales, su cesión no precisará el consentimiento de su titular.

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad

del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.

Disposición transitoria única. *Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de esta Ley.*

Los prestadores de servicios que, a la entrada en vigor de esta Ley, ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberán solicitar la anotación de, al menos, uno de ellos en el registro público en que figuraran inscritos a efectos constitutivos o de publicidad, en el plazo de un año desde la referida entrada en vigor.

Disposición final primera. *Modificación del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el párrafo a) del apartado 1 del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactada en los siguientes términos:

> »a) Que los ciudadanos puedan recibir conexión a la red telefónica pública fija y acceder a la prestación del servicio telefónico fijo disponible para el público. La conexión debe ofrecer al usuario la posibilidad de emitir y recibir llamadas nacionales e internacionales y permitir la transmisión de voz, fax y datos a velocidad suficiente para acceder de forma funcional a Internet.
>
> A estos efectos, se considerará que la velocidad suficiente a la que se refiere el párrafo anterior es la que se utiliza de manera generalizada para acceder a Internet por los abonados al servicio telefónico fijo disponible para el público con conexión a la red mediante pares de cobre y módem para banda vocal.»

Disposición final segunda. *Modificación de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el apartado 10 de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que quedará redactado como sigue:

> «10. Tasa por asignación del recurso limitado de nombres de dominio y direcciones de Internet.
>
> a) Hecho imponible.
>
> El hecho imponible de la tasa por asignación de nombres de dominio y direcciones de Internet estará constituido por la realización por la entidad pública empresarial Red.es de las actividades necesarias para la asignación y renovación de nombres de dominio y direcciones de Internet bajo el código de país correspondiente a España (.es).
>
> b) Sujetos pasivos.
>
> Serán sujetos pasivos de la tasa los solicitantes de la asignación o renovación de los nombres y direcciones de Internet.
>
> c) Cuantía.
>
> La cuantía de la tasa será única por cada nombre o dirección cuya asignación o renovación se solicite. En ningún caso se procederá a la asignación o a la renovación del nombre o dirección sin que se haya efectuado previamente el pago de la tasa.
>
> Sólo podrán modificarse mediante Ley el número e identidad de los elementos y criterios de cuantificación con base en los cuales se determinan las cuotas exigibles.
>
> A los efectos previstos en el párrafo anterior, se consideran elementos y criterios de cuantificación del importe exigible por asignación anual inicial de los nombres de dominio o direcciones de Internet el número asignado, el coste de las actividades de comprobación y verificación de las solicitudes de asignación, así como el nivel en que se produzca la asignación y, en el caso de renovación anual en los años

sucesivos, el coste del mantenimiento de la asignación y de las actividades de comprobación y de actualización de datos.

Igualmente, se atenderá al número de nombres o direcciones de Internet asignados y a la actuación a través de agentes registradores para concretar la cuantía de la tasa.

El establecimiento y modificación de las cuantías resultantes de la aplicación de los elementos y criterios de cuantificación a que se refieren los párrafos anteriores podrá efectuarse mediante Orden ministerial.

No obstante lo dispuesto en los párrafos anteriores de este apartado, en los supuestos de carácter excepcional en que así esté previsto en el Plan Nacional de Nombres de Dominio de Internet y en los términos que en el mismo se fijen, con base en el especial valor de mercado del uso de determinados nombres y direcciones, la cuantía por asignación anual inicial podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia estimado. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa. En los supuestos en que se siga este procedimiento de licitación, el Ministerio de Ciencia y Tecnología requerirá, con carácter previo a su convocatoria, a la autoridad competente para el Registro de Nombres de Dominio para que suspenda el otorgamiento de los nombres y direcciones que considere afectados por su especial valor económico. A continuación, se procederá a aprobar el correspondiente pliego de bases que establecerá, tomando en consideración lo previsto en el Plan Nacional de Nombres de Dominio de Internet, los requisitos, condiciones y régimen aplicable a la licitación.

d) Devengo.

La tasa se devengará en la fecha en que se proceda, en los términos que se establezcan reglamentariamente, a la admisión de la solicitud de asignación o de renovación de los nombres o direcciones de Internet, que no se tramitará sin que se haya efectuado el pago correspondiente.

e) Exacción y gestión recaudatoria.

La exacción de la tasa se producirá a partir de la atribución de su gestión a la entidad pública empresarial Red.es y de la determinación del procedimiento para su liquidación y pago, mediante Orden ministerial.

Los modelos de declaración, plazos y formas de pago de la tasa se aprobarán mediante resolución de la entidad pública empresarial Red.es.

El importe de los ingresos obtenidos por esta tasa se destinará a financiar los gastos de la entidad pública empresarial Red.es por las actividades realizadas en el cumplimiento de las funciones asignadas a la misma en los párrafos a), b), c) y d) del apartado 4 de esta disposición, ingresándose, en su caso, el excedente en el Tesoro Público, de acuerdo con la proporción y cuantía que se determine mediante resolución conjunta de las Secretarías de Estado de Presupuestos y Gastos y de Telecomunicaciones y para la Sociedad de la Información, a propuesta de esta última.»

Disposición final tercera. *Adición de una nueva disposición transitoria a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se añade a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, una nueva disposición transitoria duodécima, con la siguiente redacción:

«Disposición transitoria duodécima. *Criterios para el desarrollo del plan de actualización tecnológica de la red de acceso de la red telefónica pública fija.*

En el plazo máximo de cinco meses a partir de la entrada en vigor de esta disposición, el operador designado para la prestación del servicio universal presentará al Ministerio de Ciencia y Tecnología, para su aprobación en el plazo de un mes, previo informe de la Comisión del Mercado de las Telecomunicaciones, un plan de actuación detallado para garantizar que las conexiones a la red telefónica pública fija posibiliten a sus abonados el acceso funcional a Internet y, en particular, a los conectados mediante Telefonía Rural de Acceso Celular (TRAC).

El desarrollo del plan estará sujeto a las siguientes condiciones:

a) Incluirá soluciones tecnológicas eficientes disponibles en el mercado para garantizar el derecho de los usuarios a disponer, previa solicitud a partir de la aprobación del plan, de la posibilidad de acceso funcional a Internet en el plazo máximo de sesenta días desde la fecha de dicha solicitud en las zonas con cobertura. Estas soluciones tecnológicas deberán prever su evolución a medio plazo hacia velocidades de banda ancha sin que ello conlleve necesariamente su sustitución.

b) La implantación en la red de acceso de las soluciones tecnológicas a las que se refiere el párrafo a) deberá alcanzar a los abonados al servicio telefónico fijo disponible al público que, en la fecha de aprobación del plan, no tienen la posibilidad de acceso funcional a Internet, de acuerdo con el siguiente calendario:

1.º Al menos al 30 por 100 antes del 30 de junio de 2003.
2.º Al menos al 70 por 100 antes del 31 de diciembre de 2003.
3.º El 100 por 100 antes del 31 de diciembre de 2004.

En todo caso, esta implantación alcanzará, al menos, al 50 por 100 de los citados abonados en cada una de las Comunidades Autónomas antes del 31 de diciembre de 2003.

c) En el plan de actuación deberá priorizarse el despliegue al que se refiere el párrafo b) con arreglo al criterio de mayor densidad de abonados afectados.

d) A los efectos de lo dispuesto en los apartados anteriores y en caso de que sea necesario, el operador designado para la prestación del servicio universal podrá concluir con otros operadores titulares de concesiones de dominio público radioeléctrico, contratos de cesión de derechos de uso de las bandas de frecuencias necesarias para el cumplimiento de los objetivos establecidos en esta disposición. Dichos contratos deberán ser sometidos a la previa aprobación por parte del Ministerio de Ciencia y Tecnología, que podrá establecer las condiciones de salvaguarda del interés público que estime necesarias.»

Disposición final cuarta. *Modificación de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el último párrafo de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactado de la siguiente forma:

«Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango a la presente Ley se opongan a lo dispuesto en ella y, en especial, a lo dispuesto en el artículo 37.1.ª), en lo relativo a la velocidad de transmisión de datos.»

Disposición final quinta. *Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales a esta Ley.*

El Gobierno, en el plazo de un año, modificará el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, para adaptar su contenido a lo dispuesto en esta Ley.

En dicha modificación, el Gobierno tendrá especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, conforme al mandato recogido en el artículo 9.1 de la Directiva 2000/31/CE.

Disposición final sexta. *Fundamento constitucional.*

Esta Ley se dicta al amparo del artículo 149.1.6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias de las Comunidades Autónomas.

Disposición final séptima. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley.

Disposición final octava. *Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías.*

En el plazo de un año a partir de la entrada en vigor de esta Ley, el Gobierno aprobará un distintivo que permita identificar a los prestadores de servicios que respeten códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores, en los términos que reglamentariamente se establezcan.

Disposición final novena. *Entrada en vigor.*

Esta Ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

No obstante, las disposiciones adicional sexta y finales primera, segunda, tercera y cuarta de esta Ley entrarán en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

ANEXO

Definiciones

A los efectos de esta Ley, se entenderá por:

a) "Servicios de la sociedad de la información" o "servicios": todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.

2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.º La gestión de compras en la red por grupos de personas.

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.ª) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

b) "Servicio de intermediación": servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

c) "Prestador de servicios" o "prestador": persona física o jurídica que proporciona un servicio de la sociedad de la información.

d) "Destinatario del servicio" o "destinatario": persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

e) "Consumidor": persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

f) "Comunicación comercial": toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

g) "Profesión regulada": toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

h) "Contrato celebrado por vía electrónica" o "contrato electrónico": todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

i) "Ámbito normativo coordinado": todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2.º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidos en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

j) "Órgano competente": todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas.

§ 27

Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas

Ministerio de Industria, Energía y Turismo
«BOE» núm. 127, de 28 de mayo de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-5854

En el ámbito de los servicios de comunicaciones electrónicas existen agentes que desarrollan actividades destinadas a obtener un lucro económico indebido, que van desde simples usos oportunistas de las ofertas comerciales de los operadores, pasando por acciones que conllevan infracciones administrativas, hasta otras que implican actividades ilícitas, tanto relacionadas con los propios servicios de telecomunicaciones como con otros servicios conexos, como la comercialización de contenidos o los terminales y equipamientos de usuario.

Estas actividades pueden adoptar diferentes formas, que evolucionan con el tiempo, siendo las más habituales las que se aprovechan de la cadena de pagos por servicios o contenidos soportados por redes de telecomunicaciones que implican la concesión de crédito por un operador a un tercero, ya sea otro operador o un usuario final, que con frecuencia resulta impagado.

Así, estas comunicaciones suelen caracterizarse por ser generadas y prolongadas de manera artificial con el fin de obtener un lucro de la cadena de pagos de facturación. Inicialmente estas prácticas se asociaban a servicios de tarificación elevada, que ofrecen mayores márgenes de beneficio, extendiéndose sin embargo en la actualidad a todo tipo de servicios y numeraciones mediante técnicas de generación de llamadas masivas, aumentando el perjuicio económico a los operadores y usuarios y pudiendo llegar a generar problemas de calidad de servicio, e incluso poner en riesgo la seguridad y la integridad de las redes y servicios a causa de la elevada ocupación de recursos provocada.

Además, cuando estas prácticas conllevan usos no permitidos de recursos públicos de numeración, no solo constituyen una infracción de la normativa nacional específica que puede abordarse mediante un adecuado control del uso de la numeración, sino que pueden llegar a comprometer acuerdos internacionales suscritos tanto por los operadores como por el propio Reino de España cuando se realiza un uso indebido de numeración internacional.

La Comisión del Mercado de las Telecomunicaciones, organismo actualmente integrado en la Comisión Nacional de los Mercados y la Competencia, aprobó distintas resoluciones para autorizar de manera individual a los operadores para proceder al bloqueo del tráfico en determinados supuestos, así como una resolución, de 5 de septiembre de 2013, por la que se aprueba un procedimiento común para la suspensión de la interconexión de numeraciones por tráfico irregular.

El artículo 51 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones establece en su apartado segundo que, mediante real decreto, se establecerán las condiciones en las que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público lleven a cabo el bloqueo de acceso a números o servicios siempre que esté justificado por motivos de tráfico no permitido y de tráfico irregular con fines fraudulentos, y los casos en que los prestadores de servicios de comunicaciones electrónicas retengan los correspondientes ingresos por interconexión u otros servicios.

Por su parte, el artículo 19 de dicha Ley establece los principios generales de la numeración, direccionamiento y denominación de los servicios de comunicaciones electrónicas.

Por todo ello, resulta necesario adoptar medidas normativas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos, encaminadas tanto a eliminar los incentivos para estas prácticas como a asegurar el correcto uso de los recursos públicos de numeración, al tiempo que se garantiza la calidad de los servicios de comunicaciones electrónicas y, muy especialmente, la integridad y la seguridad de redes y servicios de comunicaciones electrónicas.

A los efectos del presente real decreto, existen dos tipos de tráfico no permitido, por un lado, el tráfico no permitido que usa numeración no autorizada y, por otro lado, el tráfico no permitido que hace un uso indebido de la numeración.

Se considera tráfico no permitido que usa numeración no autorizada el que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados conforme a los correspondientes planes nacionales e internacionales de numeración. Este tipo de tráfico, que se puede identificar por sus características técnicas, deberá ser bloqueado por los operadores tan pronto tengan constancia del mismo.

A su vez, el tráfico no permitido que hace un uso indebido de la numeración es aquel que, empleando numeración que sí está atribuida o habilitada y asignada, responde a usos indebidos de dicha numeración, si bien tal circunstancia no puede establecerse a priori sino tras un análisis caso por caso de sus circunstancias específicas.

Por último, se encuentra el tráfico irregular con fines fraudulentos, que es el generado, inducido o prolongado artificialmente, así como provocado a través de comunicaciones comerciales no solicitadas o mediante el control no consentido de los sistemas o terminales de usuario, al objeto de hacer un uso abusivo o fraudulento de las redes y los servicios, lo que igualmente solo puede determinarse tras un análisis caso por caso de las características específicas del tráfico.

Para todos los tipos de tráfico no permitido y tráfico irregular señalados, se establece que los operadores deben ser capaces de identificar la existencia de esta clase de tráfico en las redes que operen y en los servicios que presten, como paso previo e indispensable para llevar a cabo las debidas actuaciones contra estos tráficos, en particular cuando así les sea requerido por la Administración.

Los operadores deberán bloquear la transmisión hacia otros operadores o proveedores del tráfico no permitido que usa numeración no autorizada tan pronto como lo identifiquen, quedando obligados a identificar al menos dicho tráfico cuando es generado en sus redes y con destino en recursos de numeración pertenecientes a los planes nacionales.

Para los supuestos de tráfico no permitido que hace un uso indebido de la numeración y tráfico irregular con fines fraudulentos, se articulan actuaciones escalonadas que se inician con una solicitud del operador afectado a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información para que verifique si existe un tráfico no permitido que hace un uso indebido de la numeración o un tráfico irregular con fines fraudulentos, y autorice al bloqueo de estas comunicaciones.

Con el fin de agilizar la toma de medidas por parte de los operadores, se prevé la autorización de criterios para la puesta en funcionamiento de procedimientos específicos para que los operadores, tras una evaluación caso por caso, puedan retener los pagos relacionados con estos tráficos, así como para que puedan bloquear el tráfico dirigido a numeraciones individuales.

Tanto para el supuesto de tráfico no permitido que hace un uso indebido de la numeración como para el de tráfico irregular con fines fraudulentos, se considera la

posibilidad de que las actuaciones iniciadas por el operador tengan su origen en un conflicto entre operadores en materia de acceso o interconexión, correspondiendo en tales casos a la Comisión Nacional de los Mercados y la Competencia resolver sobre los mismos en virtud de sus competencias en la materia.

De otro lado, se prevé la posibilidad de que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información pueda adoptar medidas cautelares y requerir a los operadores para que adopten las medidas pertinentes, con el fin de garantizar la integridad y seguridad de las redes y servicios de comunicaciones electrónicas, la calidad en la prestación de servicios de comunicaciones electrónicas, o los derechos específicos de los usuarios de telecomunicaciones, entre otros objetivos, para lo que los operadores deben ser capaces de identificar el tráfico no permitido y el tráfico irregular en las redes que operen y en los servicios que presten.

Por otra parte, se prevé la adaptación de los acuerdos de acceso e interconexión entre operadores al objeto de que incorporen las disposiciones necesarias para la aplicación del presente real decreto, explicitando que la falta de adecuación de los acuerdos no exime del cumplimiento de lo establecido en el mismo, cuyas disposiciones serán efectivas desde el momento de su entrada en vigor.

Por último, se contempla que los operadores que tuvieran implantados procedimientos o sistemas previamente aprobados por la Comisión del Mercado de las Telecomunicaciones o por la Comisión Nacional de los Mercados y la Competencia para la suspensión de la interconexión de numeraciones por tráfico irregular, puedan seguir utilizándolos durante un mes tras la entrada en vigor del presente real decreto, si bien los operadores que soliciten la autorización de criterios para la implantación de sistemas o procedimientos según lo establecido en este real decreto podrán seguir utilizando dichos procedimientos previamente aprobados hasta que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva sobre esta solicitud.

Las medidas contenidas en el presente real decreto se dictan de conformidad con los artículos 19 y 20, y con el apartado 2 del artículo 51 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Este real decreto se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones, reconocida en el artículo 149.1.21.ª de la Constitución.

En su virtud, a propuesta del Ministro de Industria, Energía y Turismo, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas y de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 14 de mayo de 2015,

DISPONGO:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto establece medidas y actuaciones destinadas a prevenir y evitar el tráfico que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados; determinados tipos de tráfico contrarios a lo establecido en las disposiciones de atribución, habilitación o asignación de recursos nacionales e internacionales de numeración; así como el tráfico irregular con fines fraudulentos cursado en las redes públicas y servicios de comunicaciones electrónicas disponibles al público.

2. El presente real decreto se aplica a los operadores que exploten redes públicas de comunicaciones electrónicas o presten servicios de comunicaciones electrónicas disponibles al público.

3. Los objetivos del presente real decreto son proteger la integridad de las redes y la seguridad de las redes y servicios de comunicaciones electrónicas, asegurar la calidad en la prestación de los servicios de comunicaciones electrónicas y garantizar los derechos de los usuarios. Asimismo, se persigue reducir los perjuicios económicos sufridos tanto por los operadores como por los usuarios.

Artículo 2. *Concepto de tráfico no permitido.*

1. A los efectos del presente real decreto, existen dos tipos de tráfico no permitido:

a) Tráfico no permitido que usa numeración no autorizada.
b) Tráfico no permitido que hace un uso indebido de la numeración.

2. Se considera tráfico no permitido que usa numeración no autorizada el que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados, pertenecientes a los siguientes planes e instrucciones sobre recursos de numeración:

a) El plan nacional de numeración telefónica, aprobado mediante Real Decreto 2296/2004, de 10 de diciembre,
b) las instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, establecidas en la Orden ITC/308/2008, de 31 de enero,
c) el plan internacional de numeración descrito en la recomendación E.164 del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), incluyendo en este último caso los códigos de país o de red internacional que no hayan sido atribuidos por el UIT-T, los rangos de numeración que no hayan sido comunicados por las correspondientes autoridades nacionales a través del boletín de explotación del UIT-T, y los destinos identificados por procedimientos de marcación contrarios a lo recogido en la correspondiente lista anexa del citado boletín.
d) Cualquier otro plan de numeración que se determine por orden del Ministerio de Industria, Energía y Turismo.

3. Se considera tráfico no permitido que hace un uso indebido de la numeración el que tenga origen o destino en recursos públicos de numeración de los planes identificados en el apartado anterior que hayan sido asignados y que haga un uso de dichos recursos contrario a las condiciones de uso establecidas en las correspondientes disposiciones de atribución, habilitación o aplicación.

Artículo 3. *Concepto de tráfico irregular con fines fraudulentos.*

1. A los efectos del presente real decreto, se considera tráfico irregular el que presenta características que difieren significativamente de los patrones habituales de tráfico cursado bajo un funcionamiento ordinario de la red o de los servicios correspondiente a prácticas comerciales generalmente aceptadas en la prestación de los servicios de comunicaciones electrónicas, en aspectos tales como su volumen, número de conexiones o distribución en el tiempo, para determinados orígenes, destinos, rutas o áreas geográficas.
2. El tráfico irregular tendrá fines fraudulentos cuando resulte generado, inducido o prolongado artificialmente al objeto de obtener lucro, directo o indirecto, de la cadena de facturación de pagos en la prestación de servicios de comunicaciones electrónicas disponibles al público.
En particular tendrá dicha consideración el que, cumpliendo las condiciones anteriores, responda, entre otros, a los siguientes supuestos:

a) El basado en el agotamiento de los saldos o límites de crédito de determinados usuarios mediante comunicaciones dirigidas a rutas o destinos determinados,
b) el basado en la utilización abusiva de bonos, tarifas planas o esquemas de tarificación similares dirigidos a usuarios finales para la generación de tráfico ficticio o mediante su puesta a disposición de terceros en condiciones contrarias a lo previsto en los contratos,
c) el provocado o inducido por comunicaciones no solicitadas, o
d) el provocado mediante la manipulación o control no consentido de los sistemas o terminales de usuario.

Artículo 4. *Identificación de tráfico no permitido y tráfico irregular con fines fraudulentos.*

1. Todos los operadores deberán ser capaces de identificar el tráfico no permitido que usa numeración no autorizada, cuando tenga origen en sus redes y destino en recursos públicos de numeración a los que se refieren los apartados a), b) o d) del artículo 2.2.

2. Los operadores podrán implantar procedimientos y sistemas que, basándose en las características del tráfico, permitan identificar los tipos de tráficos que obedezcan a los conceptos recogidos en los artículos 2 y 3, y actuar sobre ellos, en particular reteniendo los correspondientes pagos de interconexión, acceso o interoperabilidad, o bloqueando la transmisión de determinados tipos de tráfico, según lo dispuesto en los artículos siguientes.

3. Mediante orden del Ministerio de Industria, Energía y Turismo se podrán establecer requisitos que deban ser satisfechos por tales procedimientos y sistemas y, en su caso, la obligatoriedad de que sean sometidos a una auditoría periódica por una entidad externa, así como los requisitos que deberán cumplir las entidades auditoras y los criterios para la realización de las auditorías.

4. Los operadores que pretendan implantar tales sistemas o procedimientos lo notificarán a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información detallando los criterios empleados para identificar los diferentes tipos de tráfico, y pondrán a su disposición toda la información sobre sus características y operativa, que deberán estar debidamente documentados y desarrollados para permitir tanto su inspección por los servicios pertinentes de la Administración, como su auditoría por una entidad externa.

5. En el plazo máximo de tres meses desde la recepción de la notificación a la que se refiere el apartado anterior, la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información dictará resolución motivada, autorizando o denegando la utilización de los criterios notificados. Dicha autorización constituye requisito previo para la puesta en funcionamiento de los citados procedimientos y sistemas.

Transcurrido el plazo al que se refiere al párrafo anterior sin que haya recaído resolución expresa, deberá entenderse desestimada la solicitud, sin perjuicio de la obligación de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de resolver expresamente.

Contra las resoluciones, que agotan la vía administrativa, se podrá interponer recurso potestativo de reposición ante el mismo órgano que la haya dictado en el plazo de un mes desde el día siguiente a su notificación, de acuerdo con los artículos 116 y 117 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien ser impugnadas directamente ante el órgano competente del orden jurisdiccional de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente a la notificación, sin que puedan ser simultáneos ambos recursos.

Asimismo, con posterioridad a la puesta en funcionamiento, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá dictar instrucciones vinculantes relativas a estos sistemas o procedimientos, destinadas a garantizar el cumplimiento efectivo de lo dispuesto en el presente real decreto o en sus disposiciones de desarrollo.

Artículo 5. *Actuaciones ante el tráfico no permitido que usa numeración no autorizada.*

Los operadores que identifiquen en sus redes o servicios tráfico no permitido que usa numeración no autorizada deberán bloquear su transmisión hacia otros operadores o proveedores, y lo notificarán a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, así como a los operadores y proveedores de servicios a los que afecte este bloqueo con los que mantengan una relación contractual.

Estas notificaciones deberán realizarse en un plazo máximo de dos días hábiles a contar desde el momento de la identificación del tráfico no permitido que usa numeración no autorizada por parte del operador. En la notificación dirigida a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, se deberá indicar el momento de la identificación del tráfico no permitido que usa numeración no autorizada así como, en su caso, información que acredite el momento en que dicho tráfico comenzó a producirse, si ambos hechos no fueron simultáneos.

Artículo 6. *Actuaciones ante el tráfico no permitido que hace un uso indebido de la numeración o el tráfico irregular con fines fraudulentos.*

1. Los operadores que identifiquen en sus redes o servicios tráfico que consideren que pueda responder al supuesto de tráfico no permitido que hace un uso indebido de la numeración o de tráfico irregular con fines fraudulentos podrán presentar una solicitud razonada requiriendo autorización para el bloqueo provisional de la transmisión de dicho tráfico, dirigida a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, bien en cualquiera de los lugares que se mencionan en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, bien a través de la sede electrónica del Ministerio de Industria, Energía y Turismo.

En dicha solicitud, el operador deberá aportar las razones así como toda la información de que disponga que justifique que el tráfico afectado debe considerarse como tráfico no permitido que hace un uso indebido de la numeración o como tráfico irregular con fines fraudulentos, incluyendo la indicación del momento de su identificación por parte del operador así como, en su caso, información que acredite el momento en que dicho tráfico comenzó a producirse, si ambos hechos no fueron simultáneos.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resolverá dichas solicitudes y notificará la resolución adoptada en un plazo máximo de tres meses, autorizando o denegando el bloqueo de la transmisión del tráfico, pudiendo a tal efecto recabar informe a la Comisión Nacional de los Mercados y la Competencia sobre el impacto del bloqueo solicitado en la regulación ex ante de los mercados, y podrá adoptar medidas cautelares autorizando al bloqueo de la transmisión del tráfico.

Transcurrido el plazo al que se refiere al párrafo anterior sin que haya recaído resolución expresa, deberá entenderse desestimada la solicitud, sin perjuicio de la obligación de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de resolver expresamente.

Contra las resoluciones, que agotan la vía administrativa, se podrá interponer recurso potestativo de reposición ante el mismo órgano que la haya dictado en el plazo de un mes desde el día siguiente a su notificación, de acuerdo con los artículos 116 y 117 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien ser impugnadas directamente ante el órgano competente del orden jurisdiccional de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente a la notificación, sin que puedan ser simultáneos ambos recursos.

2. Alternativamente a lo establecido en el apartado anterior, los operadores que identifiquen tráfico no permitido que hace un uso indebido de la numeración o tráfico irregular con fines fraudulentos mediante los procedimientos o sistemas a los que se refiere el artículo 4 podrán, tras una evaluación caso por caso, retener los pagos correspondientes al mismo, aplicando la retención desde el momento de la identificación de dicho tráfico o, en el caso de que el momento de la identificación sea posterior al de la producción, desde el momento en que acrediten que el tráfico comenzó a producirse, con un plazo de treinta días naturales anteriores a la fecha de identificación, salvo que en sus acuerdos de interconexión, acceso e interoperabilidad acuerden un plazo distinto.

Asimismo, dichos operadores, tras una evaluación caso por caso, podrán bloquear temporalmente el tráfico dirigido a numeraciones individuales que correspondan a determinados orígenes, destinos o relaciones contractuales, de conformidad con los criterios autorizados por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, según lo establecido en el artículo 4.

El operador que realice retención de pagos o bloqueo de tráfico será responsable frente a las posibles reclamaciones de los titulares de la numeración afectada por los posibles perjuicios causados por dicho bloqueo.

Cuando los operadores realicen retención de pagos o bloqueo de transmisión de tráfico según lo establecido en este apartado, lo notificarán a los operadores y proveedores de servicios a los que afecte este tráfico con los que mantengan una relación contractual, así como a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aportando en este último caso toda la información necesaria para identificar el tráfico

afectado, los criterios utilizados en su evaluación y las medidas concretas adoptadas. Estas notificaciones deberán realizarse en un plazo máximo de dos días hábiles a contar desde el momento de la identificación del tráfico por el operador. En todo momento el operador podrá aportar información complementaria o adicional que permita identificar con mayor precisión el tráfico afectado.

En el plazo máximo de tres meses a contar desde el momento en que se reciba la notificación de retención de pagos o bloqueo de transmisión de tráfico a que se refiere este apartado, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá incoar un expediente para supervisar las medidas adoptadas por el operador, a raíz del cual podrá ordenar el cese del bloqueo de la transmisión del tráfico y, en su caso, la realización del pago de las cantidades que hubiesen sido retenidas, incrementadas con el interés legal del dinero. Asimismo, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá adoptar medidas cautelares requiriendo al operador que no proceda a la retención de pagos, al bloqueo de la transmisión del tráfico o a ambas medidas simultáneamente.

3. Los operadores deberán aportar toda la información complementaria que les sea requerida por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en relación con los eventos de identificación de tráfico no permitido que hace un uso indebido de la numeración o de tráfico irregular con fines fraudulentos, o de las correspondientes medidas adoptadas, ya sea como complemento a la información que hayan remitido en las notificaciones realizadas de acuerdo con el presente artículo o en relación con notificaciones realizadas por otros operadores.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá establecer el contenido y formato en que deban presentarse las notificaciones y la información complementaria requerida.

4. Si de la tramitación de los expedientes a los que se refieren los apartados anteriores se desprende que las solicitudes o notificaciones correspondientes tienen su origen en un conflicto entre operadores en materia de acceso o interconexión, la Comisión Nacional de los Mercados y la Competencia resolverá sobre los extremos objeto del conflicto, de acuerdo con lo señalado en el artículo 15 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Artículo 7. *Medidas y actuaciones por requerimiento de la Administración.*

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá en todo momento, de oficio, conforme a los trámites procedimentales y plazos establecidos en el artículo 6.1, requerir a los operadores la aplicación de medidas de bloqueo de la transmisión de tráfico, de retención de pagos o ambas simultáneamente en relación con el tráfico no permitido o el tráfico irregular, y, en su caso, adoptar medidas cautelares, con los objetivos de:

a) Garantizar la integridad de las redes y la seguridad de las redes y servicios de comunicaciones electrónicas.

b) Garantizar la calidad en la prestación de los servicios de comunicaciones electrónicas.

c) Garantizar los derechos específicos de los usuarios de telecomunicaciones.

d) Controlar el uso de la numeración asignada, en particular para garantizar el cumplimiento de las condiciones ligadas al uso de los recursos públicos de numeración establecidas en los planes e instrucciones referidos en el artículo 2.

e) Garantizar el cumplimiento de compromisos en materia de telecomunicaciones asumidos por el Reino de España en organismos internacionales, en particular en relación con el cumplimiento de las condiciones ligadas al uso de los recursos públicos de numeración internacional descritos en la recomendación E.164 de la Unión Internacional de Telecomunicaciones.

Los operadores deberán ser capaces de identificar en las redes que operen y en los servicios que presten, el tráfico al que se refieran las citadas medidas para garantizar su cumplimiento efectivo.

Disposición adicional primera. *Duración máxima de los bloqueos de tráfico.*

Los operadores que bloqueen tráfico de acuerdo con lo establecido en el artículo 6 podrán mantener dicho bloqueo durante un período máximo de doce meses, salvo que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva estableciendo la aplicación de un plazo distinto. Transcurrido este plazo, los operadores no podrán aplicar el bloqueo. Por orden del Ministerio de Industria, Energía y Turismo podrá fijarse una duración máxima distinta, que podrá ser diferente en función del tipo de tráfico de que se trate.

Asimismo, los operadores no podrán aplicar el bloqueo si se produce un cambio en la titularidad del abonado de las numeraciones individuales afectadas y así se lo solicita el operador asignatario de las mismas, así como cuando dichas numeraciones se asignen a otro operador.

Disposición adicional segunda. *Acuerdos de interconexión, acceso e interoperabilidad.*

1. Los acuerdos de interconexión, acceso e interoperabilidad entre operadores celebrados de conformidad con lo establecido en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y en el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre, se adecuarán a lo establecido en el presente real decreto y en sus disposiciones de desarrollo.

En particular, dichos acuerdos deberán describir los procedimientos que se aplicarán para el bloqueo del tráfico, la retención de los pagos y las correspondientes notificaciones al resto de operadores o proveedores de servicios.

Mediante orden del Ministerio de Industria, Energía y Turismo se podrán establecer los requisitos que han de contemplar dichos acuerdos cuando, para asegurar el cumplimiento de lo establecido en el presente real decreto, sea necesaria la colaboración entre operadores con relaciones contractuales mayoristas.

La falta de adecuación de los acuerdos no exime del cumplimiento de lo establecido en el presente real decreto, cuyas disposiciones serán efectivas desde el momento de su entrada en vigor.

2. La Comisión Nacional de los Mercados y la Competencia entenderá de los conflictos entre operadores en la negociación de estos acuerdos.

Disposición adicional tercera. *Limitación del gasto.*

Las medidas incluidas en esta norma no podrán suponer incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición transitoria primera. *Modificación de los acuerdos de interconexión, acceso e interoperabilidad entre operadores.*

En el plazo de cuatro meses desde la entrada en vigor del presente real decreto, los operadores a los que se refiere el artículo 1 revisarán y en su caso modificarán los acuerdos de interconexión, acceso a redes y a sus recursos asociados e interoperabilidad de servicios, de acuerdo con lo establecido en la disposición adicional segunda.

Disposición transitoria segunda. *Procedimientos aprobados previamente por la Administración.*

Los operadores que tuvieran implantados procedimientos previamente aprobados por la Comisión del Mercado de las Telecomunicaciones o por la Comisión Nacional de los Mercados y la Competencia para la suspensión de la interconexión de numeraciones por tráfico irregular, podrán seguir utilizando dichos procedimientos ante la Comisión Nacional de los Mercados y la Competencia en las mismas condiciones en las que lo venían haciendo durante un mes tras la entrada en vigor del presente real decreto.

No obstante, los operadores que soliciten la autorización de criterios para la implantación de sistemas o procedimientos según lo establecido en el artículo 4 del presente real decreto

en el plazo de un mes a contar desde su entrada en vigor, podrán seguir utilizando dichos procedimientos previamente aprobados hasta que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva sobre esta solicitud.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

Disposición final segunda. *Desarrollo reglamentario y aplicación.*

El Ministro de Industria, Energía y Turismo dictará, en el ámbito de sus competencias, cuantas disposiciones y medidas sean necesarias para el desarrollo y aplicación de lo establecido en el este real decreto.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 28

Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión

Ministerio de la Presidencia
«BOE» núm. 241, de 8 de octubre de 2005
Última modificación: 25 de febrero de 2008
Referencia: BOE-A-2005-16699

El Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimiento de concesión, llevó a efecto la previsión contenida en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, para la aprobación de un distintivo de identificación de los códigos de conducta que ofrezcan determinadas garantías a los consumidores y usuarios.

La norma adoptada atribuye a la Administración General del Estado, a través del Instituto Nacional del Consumo, las competencias para los actos de concesión y retirada de este distintivo público en sus artículos 10 y 11 y en su disposición transitoria única. En los artículos 8.3 y 9 se atribuyen, en exclusiva, al Instituto Nacional del Consumo competencias relativas al seguimiento de la supervisión del cumplimiento de los códigos y de las obligaciones de las entidades promotoras de estos. La disposición final segunda, por último, atribuye al Presidente del Instituto Nacional del Consumo las competencias para adoptar las resoluciones precisas para la aplicación de lo dispuesto en dicho real decreto.

Por otra parte, en su artículo 5.2 se establece la previsión de que se favorezca e impulse la oferta al consumidor o usuario de la posibilidad de elegir, entre las lenguas oficiales de la Unión Europea, aquella en la que se han de realizar las comunicaciones comerciales, en especial, la información precontractual y el contrato.

El Consejo de Ministros ha atendido un requerimiento de incompetencia realizado por el Gobierno de la Generalidad de Cataluña que se concreta en solicitar del Gobierno de la Nación que adopte el acuerdo de derogar los artículos 5.2, 10 y 11, la disposición final segunda y las referencias al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9 del Real Decreto 292/2004, de 20 de febrero, o, subsidiariamente, el de darles nueva redacción en la que se reconozca la competencia de las comunidades autónomas respecto del procedimiento y funciones ejecutivas en ellos regulados y, en cuanto al artículo 5.2, se añada la referencia a las lenguas cooficiales en el territorio español. En efecto, en su reunión de 4 de junio de 2004, dicho órgano colegiado acordó aceptar tal requerimiento en los términos que a continuación se exponen.

En el precitado acuerdo considera el Gobierno que debe reconocerse la competencia de las comunidades autónomas respecto de los actos de concesión y de retirada del distintivo

de referencia (artículos 10 y 11 del Real Decreto 292/2004, de 20 de febrero) pues constituyen dichas concesiones actos de mera ejecución, una vez verificado el cumplimiento de los requisitos y condiciones correspondientes a los códigos de conducta que permitan su utilización y que se establecen en la norma requerida.

En consecuencia, y sin excluir la competencia de que el Estado dispone para crear o aprobar un distintivo que permita identificar aquellos prestadores de servicios de la sociedad de la información que voluntariamente se adhieran y respeten unos códigos de conducta de ámbito nacional o superior, cuyos requisitos mínimos u optativos deben ser fijados por el Estado, se debe cumplir el mandato de la disposición final octava de la Ley 34/2002, de 11 de julio, y, de acuerdo con la doctrina constitucional, considera el Gobierno que procede aceptar el requerimiento de incompetencia respecto a los artículos 10 y 11 y la disposición transitoria única y, por ende, respecto a las menciones al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9, así como en lo relativo a la disposición final segunda del real decreto requerido, por lo que procede modificar dichos preceptos para acomodarlos al reparto competencial. Se mantiene, no obstante, la comunicación al Instituto Nacional del Consumo de la información relevante a los efectos de la publicidad del distintivo o su comunicación a la Comisión de Cooperación de Consumo, en el marco de la necesaria cooperación institucional.

Por último, en cuanto a la modificación que se solicita en el requerimiento de incompetencia del tenor del ar-tículo 5.2 del real decreto requerido, considera el Gobierno que en este punto no existe una «vindicatio potestatis» propia de los conflictos positivos de competencia encaminados a eliminar transgresiones concretas y efectivas de los respectivos ámbitos competenciales, tal y como establece la jurisprudencia constitucional.

El cumplimiento de este acuerdo del Consejo de Ministros exige, en consecuencia, modificar el Real Decreto 292/2004, de 20 de febrero, para acomodar los artículos 10 y 11, y la disposición transitoria única y las menciones al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9, así como la disposición final segunda, al reparto competencial.

Para facilitar la aplicación de la norma, no obstante, se ha considerado necesario establecer en un único texto normativo la regulación del distintivo público de confianza en línea, y derogar el Real Decreto 292/2004, de 20 de febrero, cuya regulación no afectada por el requerimiento de incompetencia se incorpora a este real decreto.

En la tramitación de este real decreto se ha tenido en cuenta el parecer de las comunidades autónomas y ha sido oído el Consejo de Consumidores y Usuarios.

En su virtud, a propuesta de los Ministros de Sanidad y Consumo y de Industria, Turismo y Comercio, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación en Consejo de Ministros en su reunión del día 30 de septiembre de 2005,

D I S P O N G O :

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto tiene por objeto regular el distintivo que podrán mostrar los prestadores de servicios que se adhieran a códigos de conducta que cumplan las condiciones previstas en el capítulo II de este real decreto, en cumplimiento de lo previsto en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, este real decreto establece las condiciones que deben reunir tales códigos de conducta, la concesión y retirada del distintivo y el procedimiento aplicable.

Artículo 2. *Denominación y forma del distintivo.*

Este distintivo se denominará «distintivo público de confianza en línea». Su formato es el que figura en el anexo.

Artículo 3. *Ámbito de aplicación.*

Este real decreto se aplica a las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores que adopten códigos de conducta destinados a regular las relaciones entre prestadores de servicios de la sociedad de la información y los consumidores y usuarios, cuando la adhesión a tales códigos conceda el derecho al uso y administración del «distintivo público de confianza en línea».

Este real decreto se aplicará, asimismo, a los prestadores de servicios de la sociedad de la información que hagan uso de dicho distintivo.

CAPÍTULO II

Requisitos de los códigos de conducta

Artículo 4. *Ámbito y contenido de los códigos.*

1. Los códigos de conducta de ámbito nacional o superior regulados por este real decreto deberán estar redactados en términos claros y accesibles.

2. Además de los otros requisitos exigidos en este real decreto, los códigos de conducta deben respetar la legalidad vigente e incluir, como mínimo, con suficiente grado de precisión:

a) Las garantías concretas que ofrecen a los consumidores y usuarios que mejoren o incrementen las reconocidas por el ordenamiento jurídico.

b) Un sistema de resolución extrajudicial de conflictos de entre los previstos en el artículo 7.

c) Los compromisos específicos que asumen los prestadores de servicios adheridos en relación con los problemas concretos planteados a los consumidores y usuarios del sector, identificados según la información de los promotores del código y la que, al efecto, les faciliten las asociaciones de consumidores y las Administraciones públicas sobre las reclamaciones presentadas por los consumidores y usuarios.

d) El ámbito de las actividades del prestador de servicios sometidas al código, que, al menos, englobará alguna de las siguientes áreas: las comunicaciones comerciales o la información precontractual, la contratación y los procedimientos de solución de quejas o reclamaciones, cuando estos sean distintos de los sistemas de resolución extrajudicial de conflictos a los que se refiere el artículo 7.

3. Estos códigos de conducta deberán prever la posibilidad de adhesión al código de prestadores de servicios que no sean miembros de la entidad promotora, siempre que la actividad desarrollada por estos esté incluida en el ámbito del código.

Artículo 5. *Compromisos adicionales.*

1. Sin perjuicio de cualquier otro compromiso que puedan establecer las entidades promotoras de los códigos de conducta regulados por este real decreto, estos podrán contener previsiones específicas sobre:

a) El grado de accesibilidad a los contenidos de los consumidores y usuarios que tengan alguna discapacidad o de edad avanzada, conforme a los criterios de accesibilidad generalmente reconocidos, así como los calendarios adoptados para el establecimiento de medidas adicionales.

b) Las medidas concretas adoptadas en materia de protección de los menores y de respeto a la dignidad humana y a los valores y derechos constitucionalmente reconocidos.

c) La adhesión a códigos de conducta sobre clasificación y etiquetado de contenidos. En tales casos, deberá facilitarse información completa sobre tales códigos.

d) Las instrucciones sobre los sistemas de filtrado de contenidos utilizables en las relaciones con los prestadores de servicios.

e) Los procedimientos previstos para comprobar que los prestadores de servicios reúnen las condiciones exigidas para la adhesión al código de conducta y la utilización del distintivo.

2. Las entidades promotoras de los códigos de conducta impulsarán que los prestadores de servicios adheridos ofrezcan al consumidor o usuario la posibilidad de elegir, entre las

lenguas oficiales de la Unión Europea, la lengua en que se han de realizar las comunicaciones comerciales y, en especial, la información precontractual y el contrato.

Artículo 6. *Participación del Consejo de Consumidores y Usuarios.*

En la elaboración y modificación de los códigos de conducta regulados en este real decreto deberá darse participación al Consejo de Consumidores y Usuarios. Esta participación se articulará, como mínimo, de la siguiente forma:

a) Que, con carácter previo a la redacción del código de conducta, las entidades promotoras de este pongan en conocimiento del Consejo su voluntad de adoptarlo y soliciten la colaboración de este órgano a través del procedimiento que, en cada caso, se acuerde.

b) Que las entidades promotoras soliciten a las asociaciones de consumidores y usuarios, a través del Consejo, la identificación de los problemas específicos del sector, partiendo de las reclamaciones y consultas por ellas tramitadas, y a los efectos previstos en el artículo 4.2.c).

c) Que el Consejo no emita motivadamente un dictamen desfavorable sobre el contenido definitivo del código de conducta en el plazo de un mes desde que la entidad promotora se lo hubiera solicitado. La mera formulación de observaciones al código no supone la emisión de un dictamen desfavorable. El dictamen desfavorable únicamente podrá fundarse en el incumplimiento de los requisitos recogidos en este real decreto o en las normas de protección a los consumidores y usuarios.

Artículo 7. *Sistemas de resolución extrajudicial de conflictos.*

1. Los códigos de conducta que pretendan obtener el «distintivo público de confianza en línea» deberán establecer, como medio de solución de controversias entre los prestadores de servicios y los consumidores y usuarios, el sistema arbitral de consumo u otro sistema de resolución extrajudicial de conflictos que figure en la lista que publica la Comisión Europea sobre sistemas alternativos de resolución de conflictos con consumidores y que respete los principios establecidos por la normativa comunitaria a este respecto.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos en la medida en que lo posibilite su normativa específica y con las condiciones previstas en ella.

3. La adhesión de los prestadores de servicios a uno de los sistemas mencionados en el apartado anterior es requisito necesario para la incorporación de los prestadores de servicios a los códigos de conducta.

Artículo 8. *Supervisión del cumplimiento de los códigos de conducta por los prestadores adheridos.*

1. Los códigos de conducta deberán incluir procedimientos de evaluación independientes para comprobar el cumplimiento de las obligaciones asumidas por los prestadores de servicios adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento de evaluación que se prevea, que podrá realizarse íntegramente por medios electrónicos, deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la evaluación y sanción.

b) La sencillez, accesibilidad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código de conducta y la celeridad en todas las fases del procedimiento.

c) La audiencia del reclamado y el principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias, y podrá establecerse, en su caso, su publicidad o la suspensión o expulsión de la adhesión al código o a la entidad promotora, en el caso de que se trate de prestadores de servicios integrados en ella.

e) La notificación al denunciante de la solución adoptada.

3. Las sanciones que se impongan a los prestadores de servicios por incumplimiento de los códigos de conducta deberán notificarse trimestralmente al órgano administrativo competente para la concesión y retirada del distintivo. Cuando dichas sanciones supongan la

expulsión de la adhesión al código o la suspensión de sus derechos, la notificación deberá realizarse en el plazo de los cinco días siguientes a la adopción de la sanción.

CAPÍTULO III

Obligaciones de las entidades promotoras

Artículo 9. *Obligaciones de las entidades promotoras de los códigos de conducta.*

Las entidades promotoras de códigos de conducta regulados en este real decreto tendrán las siguientes obligaciones:

a) Administrar el «distintivo público de confianza en línea», facilitar y gestionar su utilización por los prestadores de servicios adheridos al código de conducta adoptado por ellas y que, conforme a lo previsto en el artículo 7.3, le acrediten su adhesión al sistema extrajudicial de resolución de conflictos previsto en el código de conducta. Las entidades promotoras, asimismo, deberán informar al órgano administrativo competente para la concesión y retirada del distintivo sobre las adhesiones al código de conducta de nuevos proveedores de servicios o sobre las bajas, mediante la comunicación quincenal de las variaciones producidas.

b) Mantener accesible al público información actualizada sobre las entidades promotoras, el contenido del código de conducta, los procedimientos de adhesión y de denuncia frente a posibles incumplimientos del código, los sistemas de resolución extrajudicial de conflictos que promueve el código y los prestadores de servicios adheridos a este en cada momento.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

c) Remitir al órgano administrativo competente para la concesión y retirada del distintivo una memoria anual sobre las actividades realizadas para difundir el código de conducta y promover la adhesión a este, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado, las sanciones impuestas y cualquier otro aspecto que las entidades promotoras deseen destacar.

d) Evaluar periódicamente la eficacia del código de conducta, midiendo el grado de satisfacción de los consumidores y usuarios y, en su caso, actualizar su contenido para adaptarlo a los cambios experimentados en la tecnología, en la prestación y uso de los servicios de la sociedad de la información y en la normativa que les sea aplicable.

Esta evaluación deberá contar con la participación del Consejo de Consumidores y Usuarios en los términos previstos en el artículo 6 y tendrá lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

Los resultados de la evaluación se comunicarán a la Comisión Europea y al órgano administrativo competente para la concesión y retirada del distintivo.

e) Favorecer la accesibilidad de las personas que tengan alguna discapacidad o sean de edad avanzada a toda la información disponible sobre el código de conducta.

CAPÍTULO IV

Concesión y retirada del distintivo

Artículo 10. *Órgano competente para la concesión y retirada del distintivo.*

La concesión y retirada del distintivo de confianza regulado en este real decreto, así como el ejercicio de las funciones dirigidas a velar por el mantenimiento de los requisitos que justifican su otorgamiento, corresponde al órgano competente en materia de consumo de la comunidad autónoma en que esté domiciliada la entidad promotora del código. Estas resoluciones tendrán validez en todo el territorio del Estado.

A los efectos de la publicidad del distintivo prevista en el artículo 13, estos órganos deberán comunicar al Instituto Nacional del Consumo los actos de concesión o retirada del distintivo, dándole traslado de toda la información precisa para cumplir con las obligaciones

impuestas por el citado precepto, en los cinco días siguientes a la adopción de las respectivas resoluciones. En idéntico plazo, a los efectos de la publicidad y del establecimiento de la necesaria cooperación administrativa a través de la Comisión de Cooperación de Consumo, tales órganos competentes darán traslado al Instituto Nacional del Consumo de la información que le hayan facilitado las entidades promotoras conforme a los artículos 8.3 y 9.a), c) y d).

Artículo 11. *Otorgamiento del distintivo.*

1. Las entidades promotoras de los códigos de conducta regulados en este real decreto presentarán su solicitud ante el órgano administrativo competente para la concesión y retirada del distintivo, a la que acompañarán de una copia del código, de la documentación acreditativa de la participación del Consejo de Consumidores y Usuarios y, en su caso, de haberse comunicado el proyecto de código a la Comisión Europea.

Asimismo, deberán aportar la documentación relativa a la adhesión de los prestadores de servicios que lo hayan suscrito al sistema extrajudicial de resolución de litigios que se prevea en el código.

2. En la tramitación de este procedimiento, el órgano competente para la concesión y retirada del «distintivo público de confianza en línea» podrá requerir cuantos informes estime pertinentes para valorar el alcance y contenido del código de conducta presentado y, en todo caso, con carácter preceptivo, el informe del Ministerio de Industria, Turismo y Comercio y de la Comisión de Cooperación de Consumo. En el caso de tratarse de códigos de conducta que afecten a actividades de venta a distancia deberá solicitarse el informe preceptivo de los órganos competentes en materia de inscripción, registro y control de estas empresas.

Asimismo, el órgano administrativo competente para la concesión y retirada del distintivo podrá solicitar el informe de los órganos competentes en materia de defensa de la competencia cuando, por el alcance y contenido del código, surgieran dudas sobre si puede afectar negativamente a la competencia.

3. Las resoluciones que se dicten en este procedimiento deberán ser motivadas y se publicarán en el diario oficial de la comunidad autónoma competente, conforme a lo previsto en el artículo 10, y en el «Boletín Oficial del Estado».

Dichas resoluciones serán recurribles conforme a lo previsto en el capítulo II del título VII de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 12. *Retirada del distintivo público de confianza.*

El derecho a la utilización y administración del «distintivo público de confianza en línea» podrá ser retirado si las entidades promotoras de los códigos de conducta reconocidos incumplen las obligaciones establecidas en este real decreto. La retirada del derecho a la utilización y administración del «distintivo público de confianza en línea» a una entidad promotora implicará la imposibilidad de su utilización por parte de los prestadores de servicios adheridos al código de conducta.

Asimismo, ante la inactividad de la entidad promotora y sin perjuicio de las medidas que pudieran adoptarse frente a ella por tal causa, podrá retirarse directamente el uso del distintivo a los prestadores de servicios que incumplan manifiesta y reiteradamente el código de conducta cuya adhesión les confiera tal derecho.

La retirada del distintivo de confianza se tramitará mediante un procedimiento contradictorio y contará con el informe preceptivo de la Comisión de Cooperación de Consumo; asimismo, podrá adoptarse como medida provisional la suspensión del derecho a utilizar el distintivo. La resolución por la que se retire el distintivo será recurrible conforme a lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 13. *Publicidad del distintivo.*

1. El Instituto Nacional del Consumo publicará en su página de Internet los códigos de conducta a los que se conceda el distintivo regulado en este real decreto; la relación de las entidades promotoras de dichos códigos y la de los prestadores de servicios adheridos; las

sanciones impuestas a los prestadores de servicios por incumplimiento, si son públicas, especialmente cuando lleven aparejada la suspensión o expulsión del prestador de servicios del código o de la entidad promotora o la retirada del «distintivo público de confianza en línea», y la dirección establecida para la presentación de quejas por incumplimiento de los códigos y la de los órganos de resolución extrajudicial de conflictos previstos en los códigos de conducta.

2. Las entidades promotoras de los códigos de conducta a las que se haya concedido el derecho a la utilización y administración del distintivo regulado en este real decreto y los prestadores de servicios adheridos a tales códigos podrán usar, tanto gráficamente como por su denominación, el «distintivo público de confianza en línea» en todas sus manifestaciones internas y externas, incluidas las campañas de publicidad. Todo ello sin perjuicio del cumplimiento de las obligaciones de información al consumidor, en particular, en relación con la adhesión a sistemas extrajudiciales de resolución de conflictos.

3. Las entidades promotoras y los prestadores de servicios adheridos a los códigos de conducta deberán posibilitar el acceso al contenido del código y a la dirección habilitada para presentar las quejas y reclamaciones a través de los soportes informáticos en los que se inserte el «distintivo público de confianza en línea».

CAPÍTULO V

Actuaciones de control

Artículo 14. *Actuaciones de control.*

Cuando la utilización del «distintivo público de confianza en línea», contraviniendo lo dispuesto en este real decreto, constituya publicidad ilícita, el Instituto Nacional del Consumo y los órganos competentes en materia de consumo de las comunidades autónomas podrán iniciar el procedimiento sancionador o promover el ejercicio de las acciones judiciales que procedan, de conformidad con lo previsto en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, en el Real Decreto 1945/1983, de 22 de junio, por el que se regulan las infracciones y sanciones en materia defensa del consumidor y de la producción agroalimentaria, en la Ley 34/1988, de 11 de noviembre, General de Publicidad, o en las respectivas leyes autonómicas.

Disposición transitoria primera. *Adaptación de los códigos vigentes.*

Hasta el 31 de julio de 2006, las entidades promotoras de códigos vigentes en la fecha de entrada en vigor de este real decreto podrán solicitar la concesión del «distintivo público de confianza en línea», acreditando, en su caso, que se ha comunicado el proyecto adaptado a la Comisión Europea.

En tales supuestos, no será exigible la notificación previa al Consejo de Consumidores y Usuarios prevista en el artículo 6.a), y bastará con que se requiera la colaboración de dicho órgano, a través del procedimiento que en cada caso se acuerde, para la realización de las adaptaciones precisas para cumplir los requisitos exigidos en este real decreto.

Disposición transitoria segunda. *Período transitorio.*

1. Las disposiciones de este real decreto serán de aplicación a todos los procedimientos de concesión o retirada que estén en tramitación a su entrada en vigor. A tales efectos, el Instituto Nacional del Consumo trasladará al órgano competente para la concesión o retirada del «distintivo público de confianza en línea» la documentación que obre en su poder, y se abstendrá de realizar cualquier otra actuación de impulso del procedimiento.

2. Los «distintivos públicos de confianza en línea» que se hubieran concedido conforme a la normativa aplicable con anterioridad a la entrada en vigor de este real decreto mantendrán toda su vigencia. El Instituto Nacional del Consumo trasladará al órgano competente en cada caso toda la documentación que obre en su poder respecto de tales procedimientos al objeto de que dicho órgano ejerza las funciones de vigilancia que le atribuye el artículo 10.

3. Las solicitudes que se formulen tras la entrada en vigor de este real decreto se realizarán ante el órgano competente, conforme al artículo 10.

Disposición derogatoria única. *Derogación del Real Decreto 292/2004, de 20 de febrero.*

Se deroga el Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimiento de concesión.

Disposición final primera. *Título y habilitación competencial.*

Este real decreto se dicta al amparo del artículo 149.1.1.ª, 6.ª, 8.ª y 21.ª de la Constitución y en ejecución de lo dispuesto en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

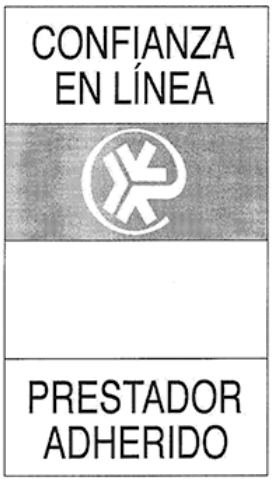
Disposición final segunda. *Facultad de aplicación.*

Los órganos competentes de las comunidades autónomas podrán adoptar las resoluciones precisas para la aplicación de lo dispuesto en este real decreto, en particular aquellas que posibiliten la gestión íntegra de los procedimientos previstos en él mediante la utilización de técnicas electrónicas, informáticas y telemáticas, de conformidad con lo previsto en la normativa vigente.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO



Denominación: Distintivo público de confianza en línea.

Construcción gráfica:

Una figura vertical constituida por cuatro rectángulos iguales de 45 mm de base por 20,25 de altura. Las medidas totales exteriores incluidos los cuatro elementos son 45 mm de base por 81 mm de altura. El segundo recuadro contiene una imagen mixta representativa de la expresión abreviada de la arroba y el logotipo de Arbitraje de Consumo.

Los rectángulos superior e inferior contienen los siguientes textos: el superior CONFIANZA EN LÍNEA y el inferior PROVEEDOR ADHERIDO, ambos en mayúsculas. El tercer recuadro, opcional, es un espacio en blanco para situar distintos logotipos.

Tipografía: helvética. Estilo: normal. Cuerpo de letra: 22. Interlineado: sólido. Escala horizontal: 100

Colores: naranja y negro. El primero compuesto por magenta 47% y amarillo 100 % y el segundo negro base. El logotipo arriba descrito figura calado en blanco sobre fondo naranja.

Si se prescinde del recuadro blanco opcional, el conjunto del logotipo.

Todas las líneas que forman el conjunto son en color negro de 0,5 puntos.

Si se prescinde del recuadro blanco opcional las medidas del conjunto del logotipo deben ser de 45 mm de base por 61 mm de altura.

Para su uso en Internet se establece un tamaño mínimo en píxeles de 75 de ancho por 134 de altura, en la versión completa y de 48 de ancho por 65 de altura prescindiendo del recuadro opcional. Se deben guardar las mismas proporciones en tamaños superiores.

§ 29

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

Jefatura del Estado
«BOE» núm. 150, de 23 de junio de 2007
Última modificación: 2 de octubre de 2015
Referencia: BOE-A-2007-12352

Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565.
Téngase en cuenta que la disposición final 7 de la citada ley establece un plazo de dos años desde su entrada en vigor para que produzcan efectos las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, y por tanto, hasta ese momento, se mantendrán en vigor los artículos de la presente ley que traten sobre las materias citadas.

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presenten vieren y entedieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

Determinadas edades de la humanidad han recibido su denominación de las técnicas que se empleaban en las mismas y hoy podríamos decir que las tecnologías de la información y las comunicaciones están afectando también muy profundamente a la forma e incluso al contenido de las relaciones de los seres humanos entre sí y de las sociedades en que se integran. El tiempo actual –y en todo caso el siglo XXI, junto con los años finales del XX–, tiene como uno de sus rasgos característicos la revolución que han supuesto las comunicaciones electrónicas. En esa perspectiva, una Administración a la altura de los tiempos en que actúa tiene que acompañar y promover en beneficio de los ciudadanos el uso de las comunicaciones electrónicas. Estos han de ser los primeros y principales beneficiarios del salto, impensable hace sólo unas décadas, que se ha producido en el campo de la tecnología de la información y las comunicaciones electrónicas. Al servicio, pues, del ciudadano la Administración queda obligada a transformarse en una administración

electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución.

Es en ese contexto en el que las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. Depende de la confianza y seguridad que genere en los ciudadanos y depende también de los servicios que ofrezca.

El mejor servicio al ciudadano constituye la razón de la reformas que tras la aprobación de la Constitución se han ido realizando en España para configurar una Administración moderna que haga del principio de eficacia y eficiencia su eje vertebrador siempre con la mira puesta en los ciudadanos. Ese servicio constituye también la principal razón de ser de la Ley de acceso electrónico de los ciudadanos a los servicios públicos que trata, además, de estar a la altura de la época actual.

En efecto, la descentralización política del Estado no se agotó en su primer y más inmediato designio de organizar políticamente España de una forma muy diferente al Estado unitario, sino que ha sido ocasión para que la mayor proximidad democrática de los nuevos poderes autonómicos se tradujese también en una mayor proximidad de las Administraciones de ellos dependientes respecto del ciudadano.

En la misma línea se mueve el reconocimiento constitucional de la autonomía local.

No obstante, esa mayor proximidad al ciudadano de la Administración, derivada de la descentralización autonómica y local, no ha acabado de superar la barrera que sigue distanciando todavía al ciudadano de la Administración, de cualquier Administración, incluida la del Estado, y que, muchas veces, no es otra que la barrera que levanta el tiempo y el espacio: el tiempo que hay que dedicar a la relación con aquélla para la realización de muchos trámites de la vida diaria que empiezan a veces por la necesidad de una primera información que exige un desplazamiento inicial, más los sucesivos desplazamientos y tiempo que se dedican a posteriores trámites a hacer con la Administración para las actividades más elementales. Esas primeras barreras potencian, en ocasiones, otras que afectan a la posición servicial de las Administraciones Públicas. Éstas no pueden cumplir siempre su misión atendiendo cualquier cosa que pida un ciudadano, puesto que puede estar en contradicción con los intereses de la mayoría de los demás ciudadanos, con los intereses generales representados por las leyes. Pero en esos casos –en que los intereses generales no coinciden con los intereses individuales– la relación con el ciudadano debe ser, también, lo más rápida y clara posible sin pérdidas de tiempo innecesarias.

En todo caso, esas primeras barreras en las relaciones con la Administración –la distancia a la que hay que desplazarse y el tiempo que es preciso dedicar– hoy día no tienen razón de ser. Las tecnologías de la información y las comunicaciones hacen posible acercar la Administración hasta la sala de estar de los ciudadanos o hasta las oficinas y despachos de las empresas y profesionales. Les permiten relacionarse con ella sin colas ni esperas. E incluso recibir servicios e informaciones ajenos a actividades de intervención administrativa o autorización; informaciones y servicios no relacionados con actuaciones limitadoras, sino al contrario ampliadoras de sus posibilidades. Esas condiciones permiten también a los ciudadanos ver a la Administración como una entidad a su servicio y no como una burocracia pesada que empieza por exigir, siempre y para empezar, el sacrificio del tiempo y del desplazamiento que impone el espacio que separa el domicilio de los ciudadanos y empresas de las oficinas públicas. Pero, además de eso, las nuevas tecnologías de la información facilitan, sobre todo, el acceso a los servicios públicos a aquellas personas que antes tenían grandes dificultades para llegar a las oficinas públicas, por motivos de localización geográfica, de condiciones físicas de movilidad u otros condicionantes, y que ahora se pueden superar por el empleo de las nuevas tecnologías. Se da así un paso trascendental para facilitar, en igualdad de condiciones, la plena integración de estas personas en la vida pública, social, laboral y cultural.

De ello se percató la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC), que en su primera versión recogió ya en su artículo 45 el impulso al empleo y aplicación de las

técnicas y medios electrónicos, informáticos y telemáticos, por parte de la Administración al objeto de desarrollar su actividad y el ejercicio de sus competencias y de permitir a los ciudadanos relacionarse con las Administraciones cuando fuese compatible con los «medios técnicos de que dispongan».

Esa previsión, junto con la de la informatización de registros y archivos del artículo 38 de la misma Ley en su versión originaria y, especialmente, en la redacción que le dio la Ley 24/2001 de 27 de diciembre al permitir el establecimiento de registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones por medios telemáticos, abría el paso a la utilización de tales medios para relacionarse con la Administración.

Simultáneamente, la misma Ley 24/2001 modificó el artículo 59 permitiendo la notificación por medios telemáticos si el interesado hubiera señalado dicho medio como preferente o consentido expresamente.

En el mismo sentido destacan las modificaciones realizadas en la Ley General Tributaria para permitir también las notificaciones telemáticas así como el artículo 96 de la nueva Ley General Tributaria de 2003 que prevé expresamente la actuación administrativa automatizada o la imagen electrónica de los documentos.

Sin embargo, el desarrollo de la administración electrónica es todavía insuficiente. La causa en buena medida se debe a que las previsiones de los artículos 38, 45 y 59 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común son facultativas. Es decir, dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo, o no, relacionarse por medios electrónicos con ellas, según que éstas quieran poner en pie los instrumentos necesarios para esa comunicación con la Administración.

Por ello esta Ley pretende dar el paso del «podrán» por el «deberán».

Las avanzadas para el momento, pero por otra parte prudentes, previsiones legales, muy válidas en 1992 o en 2001, hoy han quedado desfasadas, ante una realidad en que el grado de penetración de ordenadores y el número de personas y entidades con acceso en banda ancha a Internet, con las posibilidades abiertas a otras tecnologías y plataformas, no se corresponden ya con los servicios meramente facultativos que la Ley citada permite y estimula a establecer a las Administraciones.

El servicio al ciudadano exige consagrar su derecho a comunicarse con las Administraciones por medios electrónicos. La contrapartida de ese derecho es la obligación de éstas de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse. Esa es una de las grandes novedades de la Ley: pasar de la declaración de impulso de los medios electrónicos e informáticos –que se concretan en la práctica en la simple posibilidad de que algunas Administraciones, o algunos de sus órganos, permitan las comunicaciones por medios electrónicos– a que estén obligadas a hacerlo porque la Ley reconoce el derecho de los ciudadanos a establecer relaciones electrónicas.

La Ley consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones. El reconocimiento de tal derecho y su correspondiente obligación se erigen así en el eje central del proyecto de Ley.

Pero en torno a dicho eje es preciso abordar muchas otras que contribuyen a definir y concretar el alcance de ese derecho. Así, por ejemplo, tal derecho se hace efectivo de modo real mediante la imposición, al menos en el ámbito de la Administración General del Estado y en los términos de la ley, de la obligación de poner a disposición de ciudadanos y empresas al menos un punto de acceso general a través del cual los usuarios puedan, de forma sencilla, acceder a la información y servicios de su competencia; presentar solicitudes y recursos; realizar el trámite de audiencia cuando proceda; efectuar pagos o acceder a las notificaciones y comunicaciones que les remitan la Administración Pública.

También debe encontrar información en dicho punto de acceso único sobre los servicios multicanal o que le sean ofrecidos por más de un medio, tecnología o plataforma.

II

La Ley se articula a partir de las competencias del Estado que le reconoce el artículo 149.1.18 de la Constitución: «Bases del régimen jurídico de las Administraciones Públicas», por una parte y «procedimiento administrativo común» por otra.

Por otra parte, la regulación estatal, en lo que tiene de básico, deja margen a los desarrollos autonómicos, sin que pueda olvidarse, además, que el objeto de las bases en este caso deben permitir «en todo caso», de acuerdo con este número 18, un «tratamiento común» ante ellas.

En esta perspectiva, la regulación del Estado debe abordar aquellos aspectos en los que es obligado que las previsiones normativas sean comunes, como es el caso de la interoperabilidad, las garantías de las comunicaciones electrónicas, los servicios a los que tienen derecho los ciudadanos, la conservación de las comunicaciones electrónicas y los demás temas que se abordan en la ley para garantizar que el ejercicio del derecho a relacionarse electrónicamente con todas las administraciones forme parte de ese tratamiento común que tienen.

La Ley 30/1992 se limitó a abrir la posibilidad, como se ha dicho, de establecer relaciones telemáticas con las Administración, pero la hora actual demanda otra regulación que garantice, pero ahora de modo efectivo, un tratamiento común de los ciudadanos antes todas las Administraciones: que garantice, para empezar y sobre todo, el derecho a establecer relaciones electrónicas con todas las Administraciones Públicas. Las nuevas realidades, exigencias y experiencias que se han ido poniendo de manifiesto; el propio desarrollo de la sociedad de la información, la importancia que una regulación clara, precisa y común de los derechos de los ciudadanos y el cambio de circunstancias tecnológicas y sociales exige actualizar el contenido, muy diferente al de 1992, de la regulación básica que esté hoy a la altura de las nueva exigencias. Esa regulación común exige, hoy, por ejemplo, reconocer el derecho de los ciudadanos –y no sólo la posibilidad– de acceder mediante comunicaciones electrónicas a la Administración.

III

El reconocimiento general del derecho de acceder electrónicamente a las Administraciones Públicas tiene otras muchas consecuencias a las que hay dar solución y de las que aquí, de forma resumida, se enumeran algunas.

Así, en primer lugar, la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de unos datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal deben bastar, y no se trata de hacer ninguna innovación al respecto, pero sí de establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración.

Por otra parte, los interesados en un procedimiento tienen derecho de acceso al mismo y ver los documentos. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad.

En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta –recursos humanos y materiales– a una nueva forma de relacionarse con los ciudadanos, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y en general adaptar los procedimientos a la nueva realidad que imponen las nuevas tecnologías.

El hecho de reconocer el derecho de los ciudadanos a comunicarse electrónicamente con la Administración plantea, en primer lugar, la necesidad de definir claramente la «sede» administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad. Exige también abordar la definición a los efectos de la Ley de una serie de términos y conceptos cuyo uso habitual obliga en un contexto de comunicaciones electrónicas a efectuar muchas precisiones. Tal sucede con la definición de

expediente electrónico y de documento electrónico; de los registros electrónicos y de las notificaciones electrónicas o del alcance y sistemas de sellados de tiempo.

La consagración de ese derecho de los ciudadanos a comunicarse electrónicamente con la Administración suscita, también, por ejemplo, la cuestión de la forma de utilizar y archivar dichas comunicaciones. Y lo plantea tanto en lo que podría considerarse la formación del expediente o el archivo de oficina –el vinculado a la tramitación de los expedientes–, como en lo que se refiere al archivo de los expedientes ya tramitados.

En cuanto al funcionamiento interno de la Administración, las nuevas tecnologías permiten oportunidades de mejora (eficiencia y reducción de costes) que hacen ineludible la consideración de las formas de tramitación electrónica, tanto para la tramitación electrónica de expedientes, como para cualquier otra actuación interna de la Administración, expandiéndolas gradualmente con el objetivo del año 2009.

Ciertamente, el uso de medios electrónicos no puede significar merma alguna del derecho del interesado en un expediente a acceder al mismo en la forma tradicional, así como tampoco puede suponer un freno o un retraso para que la Administración internamente adopte los mecanismos más adecuados, en este caso medios electrónicos, que le permitan mejorar procesos y reducir el gasto público. Conjugar ambos requerimientos es posible gracias a las medidas de la política de fomento de desarrollo de la Sociedad de la Información que se vienen impulsando en los últimos años. En este sentido la Administración debe incorporar las nuevas tecnologías a su funcionamiento interno y, simultáneamente, se debe garantizar que aquellos ciudadanos que por cualquier motivo (no disponibilidad de acceso a las nuevas tecnologías o falta de formación) no puedan acceder electrónicamente a la Administración Pública, dispongan de los medios adecuados para seguir comunicándose con la Administración con los mismos derechos y garantías. La solución a ese doble objetivo pasa por la formación del personal al servicio de la Administración que atiende al público para que hagan posible la comunicación de estos ciudadanos con la administración electrónica, así como por la disponibilidad de puntos de acceso electrónico públicos en sedes administrativas. O también, desde luego, establecer las previsiones generales que sean garantía de los derechos de los ciudadanos y de un tratamiento igual ante todas las Administraciones en todos esos supuestos.

En segundo lugar es necesario regular la validez de los documentos y sus copias y la forma de que el documento electrónico opere con plena validez en modo convencional y, en su caso, la forma en que los documentos convencionales se transformen en documentos electrónicos.

Otra cuestión que se aborda es la de las plataformas que pueden utilizar los ciudadanos o las propias Administraciones para establecer tales comunicaciones electrónicas. El ordenador e Internet puede ser una vía, pero no es desde luego la única; las comunicaciones vía SMS pueden ser otra forma de actuación que en algunas Administraciones están siendo ya utilizadas. La Televisión Digital Terrestre, por ejemplo, abre también posibilidades con las que hay también que contar. La Ley no puede limitarse a regular el uso de los canales electrónicos disponibles hoy en día, ya que la gran velocidad en el desarrollo de las tecnologías de la información hacen posible la aparición de nuevos instrumentos electrónicos que pudieran aplicarse para la administración electrónica en muy poco tiempo, siendo necesario generalizar la regulación de estos canales.

La Ley debe partir del principio de libertad de los ciudadanos en la elección de la vía o canal por el que quieren comunicarse con la Administración, si bien cada tecnología puede ser apta para una función en razón de sus características y de la fiabilidad y seguridad de sus comunicaciones.

IV

Debe recordarse que el impulso de una administración electrónica supone también dar respuesta a los compromisos comunitarios y a las iniciativas europeas puestas en marcha a partir de Consejo Europeo de Lisboa y Santa Maria da Feira, continuado con sucesivas actuaciones hasta la actual comunicación de la Comisión «i2010: Una Sociedad de la Información Europea para el crecimiento y el empleo».

El impulso comunitario a la iniciativa e-Europa da la máxima importancia al desarrollo de la administración electrónica, buscando aprovechar todas las posibilidades de las nuevas tecnologías como un factor determinante del futuro económico de Europa.

En estos años de vigencia de la iniciativa e-Europa el ámbito de actuación de la administración electrónica ha crecido considerablemente en sucesivas revisiones, hasta llegar a noviembre de 2005, cuando, tras la publicación de la comunicación relativa a i2010 se aprobó, en la Cumbre de Manchester, una resolución ministerial, con objetivos concretos para el desarrollo de la administración electrónica en la Unión. Tras esta resolución se aprobó el Plan de Acción sobre administración electrónica i2010, en la que se señala que los éxitos de la administración electrónica son ya claramente visibles en varios países de la UE, estimando en 50.000 millones de euros el ahorro anual en toda la Unión que una implantación generalizada de ella podría generar.

Asimismo, el 12 de diciembre de 2006, y con objeto de avanzar en la consecución del objetivo fijado por el Consejo Europeo de Lisboa, se aprobó la Directiva 2006/123/CE, relativa a los servicios en el mercado interior.

Esta Directiva establece, entre otras obligaciones para los Estados miembros, la de facilitar por medios electrónicos acceso a los trámites relacionados con las actividades de servicios y a la información de interés tanto para los prestadores como para los destinatarios de los mismos.

Por ello, y dada la analogía de esta finalidad con el objetivo de esta Ley, se realiza en la misma una referencia expresa a la información y trámites relacionados con las actividades de servicios, de forma que los artículos 6, 7 y 8 de la Directiva pueden considerarse traspuestos por esta Ley.

Por otra parte, en el contexto internacional, también otros organismos se han interesado en la administración electrónica como forma de activar la economía y mejorar el gobierno de los países como es el caso de la OCDE, que publicó en 2004 un estudio con un título casi autodescriptivo: «La administración electrónica: Un imperativo», donde resalta los ahorros que la administración electrónica puede generar al permitirles aumentar su eficacia.

También el Consejo de Europa, desde una perspectiva más social, está analizando la administración electrónica como un motor de desarrollo. En diciembre de 2004 el Comité de Ministros adoptó una recomendación donde se señala que la administración electrónica no es asunto meramente técnico, sino de gobernanza democrática.

V

En este contexto, una Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas se justifica en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías. Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías.

Por otro lado, la legislación debe proclamar y erigirse sobre un principio fundamental como es la conservación de las garantías constitucionales y legales a los derechos de los ciudadanos y en general de las personas que se relacionan con la Administración Pública, cuya exigencia se deriva del artículo 18.4 CE, al encomendar a la ley la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales. Esta conservación exige afirmar la vigencia de los derechos fundamentales no sólo como límite, sino como vector que orienta esta reforma legislativa de acuerdo con el fin promocional consagrado en el artículo 9.2 de nuestro texto fundamental, así como recoger aquellas peculiaridades que exigen la aplicación segura de estas tecnologías. Estos derechos deben completarse con otros exigidos por el nuevo soporte electrónico de relaciones, entre los que debe estar el derecho al uso efectivo de estos medios para el desarrollo de las relaciones de las personas con la Administración. Las anteriores consideraciones cristalizan en un Estatuto del ciudadano frente a la administración electrónica que recoge un elenco no limitativo de las

posiciones del ciudadano en sus relaciones con las Administraciones Públicas, así como las garantías específicas para su efectividad.

Con este fin, la Ley crea la figura del Defensor del Usuario, que atenderá las quejas y realizará las sugerencias y propuestas pertinentes para mejorar las relaciones de ciudadanos en su trato con las Administraciones Públicas por medios electrónicos.

De otro lado, merece subrayarse el papel de vanguardia que corresponde a nuestras empresas en el desarrollo de una verdadera sociedad de la información y, por ende, de una Administración accesible electrónicamente. No en vano, la integración de las Tecnologías de la Información y las Comunicaciones (TIC's) en el día a día de la empresa, necesaria en virtud de las exigencias del entorno abierto y altamente competitivo en que operan, ha sido y es palanca impulsora para el desarrollo y creciente incorporación de esas mismas tecnologías en el actuar administrativo. Al mismo tiempo, representa una ayuda insustituible para favorecer la expansión de la «cultura electrónica» entre los trabajadores-ciudadanos.

Las empresas pueden, en tal sentido, desempeñar un papel coadyuvante clave para la consecución de los objetivos pretendidos por esta Ley. Las razones apuntadas aconsejan un tratamiento específico de aquellos procedimientos y gestiones que de forma más intensa afectan al desarrollo de la actividad empresarial.

A todo ello se debe la aprobación de esta Ley de acceso electrónico de los ciudadanos a los servicios públicos, en la que se incluyen las siguientes materias con la estructura que se recoge en los siguientes apartados.

VI

La Ley se estructura en cinco títulos, seis disposiciones adicionales, una disposición transitoria, una derogatoria y ocho finales.

En el Título Preliminar se definen el objeto y finalidades de la ley, los principios generales a los que se ajusta, así como su ámbito de aplicación. Debe destacarse el carácter básico de la ley en los términos establecidos en la disposición final primera, siendo por tanto de aplicación a todas las Administraciones Públicas los artículos referidos en dicha disposición final.

La Ley establece entre otros, el principio de igualdad, para que la utilización de comunicaciones electrónicas con las Administraciones Públicas no implique una discriminación para los ciudadanos que se relacionen con la Administración por medios no electrónicos.

En el Título Primero están recogidos los derechos de los ciudadanos en sus relaciones con las Administraciones Públicas a través de medios electrónicos. Para garantizar el pleno ejercicio de estos derechos, se establece la obligación de las Administraciones de habilitar diferentes canales o medios para la prestación de los servicios electrónicos.

Asimismo, se establece la obligación de cada Administración de facilitar a las otras Administraciones los datos de los interesados que se le requieran y obren en su poder, en la tramitación de un procedimiento, siempre que el interesado preste su consentimiento expreso, el cual podrá emitirse y recabarse por medios electrónicos, al objeto de que los ciudadanos no deban aportar datos y documentos que están en poder de las Administraciones Públicas.

Para velar por la efectividad de los derechos reconocidos a los ciudadanos se prevé, en el ámbito de la Administración General del Estado, la actuación de las Inspecciones Generales de Servicios de los Departamentos Ministeriales y del Defensor del usuario.

En el Título Segundo se regula el régimen jurídico de la administración electrónica. Por una parte, su Capítulo Primero se dedica a la sede electrónica, como dirección electrónica cuya gestión y administración corresponde a una Administración Pública funcionando con plena responsabilidad respecto de la integridad, veracidad y actualización de la información y los servicios a los que puede accederse a través de la misma. En la normativa de desarrollo de la Ley, cada Administración determinará los instrumentos de creación de las sedes electrónicas.

En su Capítulo Segundo se regulan las formas de identificación y autenticación, tanto de los ciudadanos como de los órganos administrativos en el ejercicio de sus competencias, siendo destacable que se habilitan distintos instrumentos de acreditación, que se concretarán en la normativa aplicable a cada supuesto con criterios de proporcionalidad. El

Documento Nacional de Identidad electrónico está habilitado con carácter general para todas las relaciones con las Administraciones Públicas, y por ello se impulsará como fórmula para extender el uso general de la firma electrónica. También se establece la obligación para cualquier Administración de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica.

Interesa también destacar sobre esta cuestión, y con objeto de evitar la brecha digital, la posibilidad de que sean funcionarios públicos quienes acrediten la voluntad de los ciudadanos, siguiendo el procedimiento establecido, para sus relaciones electrónicas con la Administración.

En el Capítulo Tercero se regulan los registros, comunicaciones y notificaciones electrónicas. La principal novedad a este respecto es la nueva regulación de los registros electrónicos, de manera que puedan convertirse en un instrumento que se libere de la rigidez actual y sirvan para la presentación de cualquier escrito o solicitud ante las Administraciones Públicas.

La Ley regula las comunicaciones electrónicas de los ciudadanos con las Administraciones y de éstas entre sí, para aunar los criterios de agilidad y de seguridad jurídica. En el Capítulo Cuarto, sobre los documentos y archivos electrónicos, se establecen las condiciones para reconocer la validez de un documento electrónico, se regula todo el sistema de copias electrónicas, tanto las realizadas a partir de documentos emitidos originariamente en papel, como las copias de documentos que ya estuvieran en soporte electrónico y las condiciones para realizar en soporte papel copia de originales emitidos por medios electrónicos, o viceversa.

El Título Tercero trata de la gestión electrónica de los procedimientos, desarrolla la regulación de los procedimientos administrativos utilizando medios electrónicos y los criterios a seguir en la gestión electrónica, guardando un cierto paralelismo con la regulación que encontramos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Así, se regula la iniciación, instrucción y terminación de procedimientos por medios electrónicos.

En este Título cabe hacer especial referencia a la obligación que se establece para las Administraciones Públicas de poner a disposición de los usuarios información por medios electrónicos sobre el estado de tramitación de los procedimientos, tanto para los gestionados en su totalidad por medios electrónicos como para el resto de procedimientos.

El Título Cuarto está dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En él se establecen el órgano de cooperación en esta materia de la Administración General del Estado con los de las Comunidades Autónomas y con la Administración Local, y se determinan los principios para garantizar la interoperabilidad de sistemas de información así como las bases para impulsar la reutilización de aplicaciones y transferencia de tecnologías entre Administraciones.

La Ley consta, por último, de seis disposiciones adicionales, una transitoria, una derogatoria y ocho finales entre las que presenta especial relevancia la disposición final primera en la que se citan los preceptos de la ley que tienen carácter básico al amparo del artículo 149.1.18 de la Constitución.

Especial interés tiene también la disposición final tercera, pues con independencia de la fecha de entrada en vigor de la Ley, en ella se señalan las fechas para la efectividad plena del derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, estableciendo los plazos que se consideran adecuados para llevar a cabo las necesarias actuaciones previas de adecuación por parte de las distintas Administraciones Públicas.

TÍTULO PRELIMINAR

Del ámbito de aplicación y los principios generales

Artículo 1. *Objeto de la Ley.*

1. La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la

utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley, en los términos expresados en su disposición final primera, será de aplicación:

a) A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

b) A los ciudadanos en sus relaciones con las Administraciones Públicas.

c) A las relaciones entre las distintas Administraciones Públicas.

2. La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado.

Artículo 3. *Finalidades de la Ley.*

Son fines de la presente Ley:

1. Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.

2. Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.

3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.

5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.

6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.

7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.

Artículo 4. *Principios generales.*

La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios:

a) El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

b) Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se

relacionen con las Administraciones Públicas por medios no electrónicos, tanto respecto al acceso a la prestación de servicios públicos como respecto a cualquier actuación o procedimiento administrativo sin perjuicio de las medidas dirigidas a incentivar la utilización de los medios electrónicos.

c) Principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.

d) Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

e) Principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar tanto la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas como, en su caso, la prestación conjunta de servicios a los ciudadanos. En particular, se garantizará el reconocimiento mutuo de los documentos electrónicos y de los medios de identificación y autenticación que se ajusten a lo dispuesto en la presente Ley.

f) Principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

g) Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

h) Principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos.

i) Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

j) Principio de simplificación administrativa, por el cual se reduzcan de manera sustancial los tiempos y plazos de los procedimientos administrativos, logrando una mayor eficacia y eficiencia en la actividad administrativa.

k) Principio de transparencia y publicidad del procedimiento, por el cual el uso de medios electrónicos debe facilitar la máxima difusión, publicidad y transparencia de las actuaciones administrativas.

Artículo 5. *Definiciones.*

A efectos de la presente ley, los términos que en ellas se emplean tendrán el sentido que se establece en su anexo.

TÍTULO PRIMERO

Derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos

Artículo 6. *Derechos de los ciudadanos.*

1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.

b) A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.

c) A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.

d) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.

e) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.

f) A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.

g) A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.

h) A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.

i) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

j) A la calidad de los servicios públicos prestados por medios electrónicos.

k) A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

3. En particular, en los procedimientos relativos al acceso a una actividad de servicios y su ejercicio, los ciudadanos tienen derecho a la realización de la tramitación a través de una ventanilla única, por vía electrónica y a distancia, y a la obtención de la siguiente información a través de medios electrónicos, que deberá ser clara e inequívoca:

a) Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.

b) Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como los datos de las asociaciones y organizaciones distintas

de las autoridades competentes a las que los prestadores o destinatarios puedan dirigirse para obtener asistencia o ayuda.

c) Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios.

d) Las vías de reclamación y recurso en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores.

Artículo 7. *Defensa de los derechos de los ciudadanos.*

1. En la Administración General del Estado, se crea la figura del Defensor del usuario de la administración electrónica, que velará por la garantía de los derechos reconocidos a los ciudadanos en la presente Ley, sin perjuicio de las competencias atribuidas en este ámbito a otros órganos o entidades de derecho público. Será nombrado por el Consejo de Ministros a propuesta del Ministro de Administraciones Públicas entre personas de reconocido prestigio en la materia. Estará integrado en el Ministerio de Administraciones Públicas y desarrollará sus funciones con imparcialidad e independencia funcional.

2. El Defensor del usuario de la administración electrónica elaborará, con carácter anual, un informe que se elevará al Consejo de Ministros y se remitirá al Congreso de los Diputados. Dicho informe contendrá un análisis de las quejas y sugerencia recibidas así como la propuesta de las actuaciones y medidas a adoptar en relación con lo previsto en el apartado 1 de este artículo.

3. Para el ejercicio de sus funciones, el Defensor del usuario de la administración electrónica contará con los recursos de la Administración General del Estado con la asistencia que, a tal efecto, le presten las Inspecciones Generales de los Servicios de los Departamentos ministeriales y la Inspección General de Servicios de la Administración Pública. En particular, las Inspecciones de los Servicios le asistirán en la elaboración del informe al que se refiere el apartado anterior y le mantendrán permanentemente informado de las quejas y sugerencias que se reciban en relación con la prestación de servicios públicos a través de medios electrónicos. A estos efectos, la Comisión Coordinadora de las Inspecciones generales de servicios de los departamentos ministeriales realizará, en este ámbito, las funciones de coordinación que tiene legalmente encomendadas.

4. Reglamentariamente se determinará el estatuto del Defensor del usuario de la administración electrónica, así como la regulación de sus relaciones con los órganos a los que se refiere el apartado anterior de este artículo.

Artículo 8. *Garantía de prestación de servicios y disposición de medios e instrumentos electrónicos.*

1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

2. La Administración General del Estado garantizará el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

a) Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Puntos de acceso electrónico, consistentes en sedes electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos,

con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

c) Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores.

Artículo 9. *Transmisiones de datos entre Administraciones Públicas.*

1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b) de la presente Ley.

TÍTULO SEGUNDO

Régimen jurídico de la administración electrónica

CAPÍTULO I

De la sede electrónica

Artículo 10. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Artículo 11. *Publicaciones electrónicas de Boletines Oficiales.*

1. La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.

2. La publicación del «Boletín Oficial del Estado» en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

Artículo 12. *Publicación electrónica del tablón de anuncios o edictos.*

La publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente.

CAPÍTULO II

De la identificación y autenticación

Sección 1.ª Disposiciones comunes

Artículo 13. *Formas de identificación y autenticación.*

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos.

Las Administraciones Públicas deberán admitir todos los certificados reconocidos incluidos en la "Lista de confianza de prestadores de servicios de certificación" (TSL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.

b) Sistemas de firma electrónica para la actuación administrativa automatizada.

c) Firma electrónica del personal al servicio de las Administraciones Públicas.

d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Sección 2.ª Identificación de los ciudadanos y autenticación de su actuación

Artículo 14. *Utilización del Documento Nacional de Identidad.*

Las personas físicas podrán, en todo caso y con carácter universal, utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad en su relación por medios electrónicos con las Administraciones Públicas. El régimen de utilización y efectos de dicho documento se regirá por su normativa reguladora.

Artículo 15. *Utilización de sistemas de firma electrónica avanzada.*

1. Los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, referidos en el artículo 14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

2. **(Suprimido)**

3. Los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen.

Artículo 16. *Utilización de otros sistemas de firma electrónica.*

1. Las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.

2. En aquellos supuestos en los que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública, ésta deberá garantizar la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos.

3. Cuando resulte preciso, las Administraciones Públicas certificarán la existencia y contenido de las actuaciones de los ciudadanos en las que se hayan usado formas de identificación y autenticación a que se refiere este artículo.

Sección 3.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 17. *Identificación de las sedes electrónicas.*

Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.

Artículo 18. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Los certificados electrónicos a los que se hace referencia en el apartado 1.a) incluirán el número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

3. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Artículo 19. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 17 y 18, la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados.

2. Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. La firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse a los efectos de este artículo.

Artículo 20. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Sección 4.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos

Artículo 21. *Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos.*

1. Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

2. Los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.

3. La Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones. Cada Administración Pública podrá disponer de los mecanismos necesarios para la verificación del estado de revocación y la firma con los certificados electrónicos admitidos en su ámbito de competencia.

Artículo 22. *Identificación y autenticación de los ciudadanos por funcionario público.*

1. En los supuestos en que para la realización de cualquier operación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 13 de los que aquel no disponga, tal identificación o autenticación podrá ser validamente realizada por funcionarios públicos mediante el uso del sistema de firma electrónica del que estén dotados.

2. Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

3. Cada Administración Pública mantendrá actualizado un registro de los funcionarios habilitados para la identificación o autenticación regulada en este artículo.

Artículo 23. *Formas de Representación.*

Sin perjuicio de lo dispuesto en el artículo 13.2, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación.

CAPÍTULO III

De los registros, las comunicaciones y las notificaciones electrónicas

Sección 1.ª De los Registros

Artículo 24. *Registros electrónicos.*

1. Las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

2. Los registros electrónicos podrán admitir:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

3. En cada Administración Pública existirá, al menos, un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública. Las Administraciones Públicas podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio.

4. En el ámbito de la Administración General del Estado se automatizarán las oficinas de registro físicas a las que se refiere el artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, a fin de garantizar la interconexión de todas sus oficinas y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Artículo 25. *Creación y funcionamiento.*

1. Las disposiciones de creación de registros electrónicos se publicarán en el Diario Oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles a los efectos previstos en el artículo siguiente.

2. En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones a las que se refiere el apartado 2.a) del artículo anterior que pueden presentarse en el mismo así como, en su caso, la posibilidad de

presentación de solicitudes, escritos y comunicaciones a los que se refiere el apartado 2.b) de dicho artículo.

3. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

4. Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.

Artículo 26. *Cómputo de plazos.*

1. Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las Administraciones Públicas por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.

2. Los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas.

3. A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado 2.b del artículo 24, por la fecha y hora de entrada en el registro del destinatario. En todo caso, la fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el escrito, solicitud o comunicación.

5. Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. En todo caso, no será de aplicación a los registros electrónicos lo dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 27. *Comunicaciones electrónicas.*

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de Ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.

2. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.

3. Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.

4. Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas.

5. Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.

6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

7. Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes.

Artículo 28. *Práctica de la notificación por medios electrónicos.*

1. Para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización, sin perjuicio de lo dispuesto en el artículo 27.6. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados anteriormente podrán emitirse y recabarse, en todo caso, por medios electrónicos.

2. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.

3. Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992 de Régimen Jurídico y del Procedimiento Administrativo Común y normas concordantes, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.

4. Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de Régimen Jurídico y del Procedimiento Administrativo Común, excepto en los casos previstos en el artículo 27.6 de la presente Ley.

5. Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dichos acceso.

CAPÍTULO IV

De los documentos y los archivos electrónicos

Artículo 29. *Documento administrativo electrónico.*

1. Las Administraciones Públicas podrán emitir validamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección 3.ª del Capítulo II de la presente Ley.

2. Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

3. La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

Artículo 30. *Copias electrónicas.*

1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones

Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

2. Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

5. Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Artículo 31. *Archivo electrónico de documentos.*

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Artículo 32. *Expediente electrónico.*

1. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

3. La remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo.

TÍTULO TERCERO

De la gestión electrónica de los procedimientos

CAPÍTULO I

Disposiciones comunes

Artículo 33. *Utilización de medios electrónicos.*

1. La gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa.

2. En la aplicación de medios electrónicos a la actividad administrativa se considerará la adecuada dotación de recursos y medios materiales al personal que vaya a utilizarlos, así como la necesaria formación acerca de su utilización.

Artículo 34. *Criterios para la gestión electrónica.*

La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación.

b) La previsión de medios e instrumentos de participación, transparencia e información.

c) La reducción de los plazos y tiempos de respuesta.

d) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas.

CAPÍTULO II

Utilización de medios electrónicos en la tramitación del procedimiento

Artículo 35. *Iniciación del procedimiento por medios electrónicos.*

1. La iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado i) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos.

3. Con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones e, incluso,

ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el ciudadano verifique la información y, en su caso, la modifique y complete.

Artículo 36. *Instrucción del procedimiento utilizando medios electrónicos.*

1. Las aplicaciones y sistemas de información utilizados para la instrucción por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación de los órganos responsables de los procedimientos así como la tramitación ordenada de los expedientes y facilitar la simplificación y la publicidad de los procedimientos.

2. Los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre los órganos y unidades intervinientes a efectos de emisión y recepción de informes u otras actuaciones deberán cumplir los requisitos establecidos en esta Ley.

3. Cuando se utilicen medios electrónicos para la participación de los interesados en la instrucción del procedimiento a los efectos del ejercicio de su derecho a presentar alegaciones en cualquier momento anterior a la propuesta de resolución o en la práctica del trámite de audiencia cuando proceda, se emplearán los medios de comunicación y notificación previstos en los artículos 27 y 28 de esta Ley.

Artículo 37. *Acceso de los interesados a la información sobre el estado de tramitación.*

1. En los procedimientos administrativos gestionados en su totalidad electrónicamente, el órgano que tramita el procedimiento pondrá a disposición del interesado un servicio electrónico de acceso restringido donde éste pueda consultar, previa identificación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.

2. En el resto de los procedimientos se habilitarán igualmente servicios electrónicos de información del estado de la tramitación que comprendan, al menos, la fase en la que se encuentra el procedimiento y el órgano o unidad responsable.

Artículo 38. *Terminación de los procedimientos por medios electrónicos.*

1. La resolución de un procedimiento utilizando medios electrónicos garantizará la identidad del órgano competente mediante el empleo de alguno de los instrumentos previstos en los artículos 18 y 19 de esta Ley.

2. Podrán adoptarse y notificarse resoluciones de forma automatizada en aquellos procedimientos en los que así esté previsto.

Artículo 39. *Actuación administrativa automatizada.*

En caso de actuación automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

TÍTULO CUARTO

Cooperación entre administraciones para el impulso de la administración electrónica

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 40. *Comité Sectorial de administración electrónica.*

1. El Comité Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General del Estado, de las administraciones de las Comunidades Autónomas y de las entidades que integran la Administración Local en materia de administración electrónica.

2. El Comité Sectorial de la administración electrónica velará por el cumplimiento de los fines y principios establecidos en esta Ley, y en particular desarrollará las. siguientes funciones:

a) Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.

b) Preparar planes programas conjuntos de actuación para impulsar el desarrollo de la administración electrónica en España.

c) Asegurar la cooperación entre las administraciones públicas para proporcionar al ciudadano información administrativa clara, actualizada e inequívoca.

3. Cuando por razón de las materias tratadas resulte de interés podrá invitarse a las organizaciones, corporaciones o agentes sociales que se estime conveniente en cada caso a participar en las deliberaciones del comité sectorial.

CAPÍTULO II

Cooperación en materia de interoperabilidad de sistemas y aplicaciones

Artículo 41. *Interoperabilidad de los Sistemas de Información.*

Las Administraciones Públicas utilizarán las tecnologías de la información en sus relaciones con las demás administraciones y con los ciudadanos, aplicando medidas informáticas, tecnológicas, organizativas, y de seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 42. *Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.*

1. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

4. En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

Artículo 43. *Red de comunicaciones de las Administraciones Públicas españolas.*

La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

Artículo 44. *Red integrada de Atención al Ciudadano.*

1. Las Administraciones Públicas podrán suscribir convenios de colaboración con objeto de articular medidas e instrumentos de colaboración para la implantación coordinada y normalizada de una red de espacios comunes o ventanillas únicas.

2. En particular, y de conformidad con lo dispuesto en el apartado anterior, se implantarán espacios comunes o ventanillas únicas para obtener la información prevista en el artículo 6.3 de esta Ley y para realizar los trámites y procedimientos a los que hace referencia el apartado a) de dicho artículo.

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías

Artículo 45. *Reutilización de sistemas y aplicaciones de propiedad de la Administración.*

1. Las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier Administración sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente la incorporación de los ciudadanos a la Sociedad de la información

Artículo 46. *Transferencia de tecnología entre Administraciones.*

1. Las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo de la administración electrónica y de conformidad con lo que al respecto se establezca en el Esquema Nacional de Interoperabilidad.

2. La Administración General del Estado, a través de un centro para la transferencia de la tecnología, mantendrá un directorio general de aplicaciones para su reutilización, prestará asistencia técnica para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes de especial interés para el desarrollo de la administración electrónica en el marco de los esquemas nacionales de interoperabilidad y seguridad.

Disposición adicional primera. *Reunión de Órganos colegiados por medios electrónicos.*

1. Los órganos colegiados podrán constituirse y adoptar acuerdos utilizando medios electrónicos, con respeto a los trámites esenciales establecidos en los artículos 26 y el 27.1

de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. En la Administración General del Estado, lo previsto en el apartado anterior se efectuará de acuerdo con las siguientes especialidades:

a) Deberá garantizarse la realización efectiva de los principios que la legislación establece respecto de la convocatoria, acceso a la información y comunicación del orden del día, en donde se especificarán los tiempos en los que se organizarán los debates, la formulación y conocimiento de las propuestas y la adopción de acuerdos.

b) El régimen de constitución y adopción de acuerdos garantizará la participación de los miembros de acuerdo con las disposiciones propias del órgano.

c) Las actas garantizarán la constancia de las comunicaciones producidas así como el acceso de los miembros al contenido de los acuerdos adoptados.

Disposición adicional segunda. *Formación de empleados públicos.*

La Administración General del Estado promoverá la formación del personal a su servicio en la utilización de medios electrónicos para el desarrollo de las actividades propias de aquélla.

En especial, los empleados públicos de la Administración General del Estado recibirán formación específica que garantice conocimientos actualizados de las condiciones de seguridad de la utilización de medios electrónicos en la actividad administrativa, así como de protección de los datos de carácter personal, respeto a la propiedad intelectual e industrial y gestión de la información.

Disposición adicional tercera. *Plan de Medios en la Administración General del Estado.*

En el plazo de seis meses a partir de la publicación de esta Ley, el Ministerio de Administraciones Públicas, en colaboración con los Ministerios de Economía y Hacienda y de Industria, Turismo y Comercio, elevará al Consejo de Ministros un Plan de implantación de los medios necesarios para el ámbito de la Administración General del Estado. Dicho Plan incorporará las estimaciones de los recursos económicos, técnicos y humanos que se consideren precisos para la adecuada aplicación de lo dispuesto en la presente Ley en los tiempos establecidos en el calendario al que se refiere el apartado 2 de la disposición final tercera, así como los mecanismos de evaluación y control de su aplicación.

Disposición adicional cuarta. *Procedimientos Especiales.*

La aplicación de lo dispuesto en el Título Tercero de esta ley a los procedimientos en materia tributaria, de seguridad social y desempleo y de régimen jurídico de los extranjeros en España, se efectuará de conformidad con lo establecido en las disposiciones adicionales quinta, sexta, séptima y decimonovena de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Asimismo, en la aplicación de esta ley habrán de ser tenidas en cuenta las especificidades en materia de contratación pública, conforme a lo preceptuado en la disposición adicional séptima del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto Legislativo 2/2000, de 16 de junio.

Disposición adicional quinta. *Función Estadística.*

Lo dispuesto en los artículos 6.2.b) y 9 de la presente ley no será de aplicación a la recogida de datos prevista en el Capítulo II de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Disposición adicional sexta. *Uso de Lenguas Oficiales.*

1. Se garantizará el uso de las lenguas oficiales del Estado en las relaciones por medios electrónicos de los ciudadanos con las Administraciones Públicas, en los términos previstos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en la normativa que en cada caso resulte de aplicación.

2. A estos efectos, las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

3. Los sistemas y aplicaciones utilizados en la gestión electrónica de los procedimientos se adaptarán a lo dispuesto en cuanto al uso de lenguas cooficiales en el artículo 36 de la ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común.

4. Cada Administración Pública afectada determinará el calendario para el cumplimiento progresivo de lo previsto en la presente disposición, debiendo garantizar su cumplimiento total en los plazos establecidos en la disposición final tercera.

Disposición transitoria única. *Régimen Transitorio.*

1. Los procedimientos y actuaciones de los ciudadanos y las Administraciones Públicas que, utilizando medios electrónicos, se hayan iniciado con anterioridad a la entrada en vigor de la presente Ley se seguirán rigiendo por la normativa anterior hasta su terminación.

2. Los registros telemáticos existentes a la entrada en vigor de la presente Ley serán considerados registros electrónicos regulándose por lo dispuesto en los artículos 24, 25 y 26 de esta Ley.

Disposición derogatoria única.

1. Quedan derogados los siguientes preceptos de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común: apartado número 9 del artículo 38, apartados números 2, 3 y 4 del artículo 45, apartado número 3 del artículo 59 y la disposición adicional decimoctava.

2. Asimismo, quedan derogadas las normas de igual o inferior rango en cuanto contradigan o se opongan a lo dispuesto en la presente Ley.

Disposición final primera. *Carácter básico de la Ley.*

1. Los artículos 1, 2, 3, 4, 5, 6, 8.1, 9, 10, 11.1, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21.1,21.2, 22, 23, 24.1, 24.2, 24.3, 25, 26, 27, 28, 29.1, 29.2, 30, 32, 35, 37.1, 38, 42, el apartado 1 de la disposición adicional primera, la disposición adicional cuarta, la disposición transitoria única y la disposición final tercera se dictan al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas y sobre el procedimiento administrativo común.

2. Con excepción del artículo 42, el Título IV de la presente ley será de aplicación a todas las Administraciones Públicas en la medida en que éstas participen o se adscriban a los órganos de cooperación o instrumentos previstos en el mismo.

Disposición final segunda. *Publicación electrónica del «Boletín Oficial del Estado».*

La publicación electrónica del «Boletín Oficial del Estado» tendrá el carácter y los efectos previstos en el artículo 11.2 de la presente Ley desde el 1 de enero de 2009.

Disposición final tercera. *Adaptación de las Administraciones Públicas para el ejercicio de derechos.*

1. Desde la fecha de entrada en vigor de la presente Ley, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con los procedimientos y actuaciones adaptados a lo dispuesto en la misma, sin perjuicio de lo señalado en los siguientes apartados. A estos efectos, cada Administración Pública hará pública y mantendrá actualizada la relación de dichos procedimientos y actuaciones.

2. En el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009. A tal fin, el Consejo de Ministros

establecerá y hará público un calendario de adaptación gradual de aquellos procedimientos y actuaciones que lo requieran.

3. En el ámbito de las Comunidades Autónomas, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias.

4. En el ámbito de las Entidades que integran la Administración Local, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del 31 de diciembre de 2009 siempre que lo permitan sus disponibilidades presupuestarias. A estos efectos las Diputaciones Provinciales, o en su caso los Cabildos y Consejos Insulares u otros organismos supramunicipales, podrán prestar los servicios precisos para garantizar tal efectividad en el ámbito de los municipios que no dispongan de los medios técnicos y organizativos necesarios para prestarlos.

5. Las Comunidades Autónomas y las Entidades integradas en la Administración Local en las que no puedan ser ejercidos a partir del 31 de diciembre de 2009 los derechos reconocidos en el artículo 6 de la presente Ley, en relación con la totalidad de los procedimientos y actuaciones de su competencia, deberán aprobar y hacer públicos los programas y calendarios de trabajo precisos para ello, atendiendo a las respectivas previsiones presupuestarias, con mención particularizada de las fases en las que los diversos derechos serán exigibles por los ciudadanos.

Los anteriores programas podrán referirse a una pluralidad de municipios cuando se deban ejecutar en aplicación de los supuestos de colaboración previstos en el apartado anterior.

Disposición final cuarta. *Modificación de la Ley 84/1978, de 28 de diciembre, por la que se regula la tasa por expedición del Documento Nacional de Identidad.*

Uno. El apartado 2 del artículo 4 queda redactado del siguiente modo:

> «2. Quienes hubieran de renovar preceptivamente su documento durante el plazo de vigencia del mismo, por variación de alguno de los datos que se recogen en el mismo.»

Dos. El artículo 6 queda redactado del siguiente modo:

> **«Artículo 6.** *Cuota tributaria.*
>
> La cuota tributaria exigible será de 6,70 euros. Los excesos del costo de la expedición, si existen, serán sufragados con cargo a los Presupuestos Generales del Estado.»

Disposición final quinta. *Modificación de la Ley 16/1979, de 2 de octubre, sobre Tasas de la Jefatura Central de Tráfico.*

Uno. En el apartado 1 del artículo 5 se modifica la letra d) y se incorpora una nueva letra e) que quedan redactadas del siguiente modo:

> «d) Quienes soliciten duplicados de las autorizaciones administrativas para conducir o para circular por cambio de domicilio.
>
> e) Quienes soliciten la baja definitiva de un vehículo por entrega en un establecimiento autorizado para su destrucción.»

Dos. Los puntos 4 y 4 bis, primera columna de la izquierda del Grupo IV del artículo 6, quedan redactados del siguiente modo:

> «4. Duplicados de permisos, autorizaciones por extravío, sustracción, deterioro, prórroga de vigencia o cualquier modificación de aquéllos.
>
> 4 bis. duplicados de licencias de conducción y de circulación de ciclomotores por extravío, sustracción, deterioro, prórroga de vigencia o cualquier modificación de aquéllos.»

Disposición final sexta. *Habilitación para la regulación del teletrabajo en la Administración General del Estado.*

El Ministerio de Administraciones Públicas, en colaboración con los Ministerios de Economía y Hacienda, de Industria, Turismo y Comercio y de Trabajo y Asuntos Sociales, regularán antes del 1 de marzo de 2008 las condiciones del teletrabajo en la Administración General del Estado.

Disposición final séptima. *Desarrollo reglamentario del artículo 4.c).*

El Gobierno desarrollará reglamentariamente lo previsto en el artículo 4.c) de la presente Ley para garantizar que todos los ciudadanos, con especial atención a las personas con algún tipo de discapacidad y mayores, que se relacionan con la Administración General del Estado puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos.

Disposición final octava. *Desarrollo y entrada en vigor de la Ley.*

1. Corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de la presente Ley.
2. La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Definiciones

A efectos de la presente ley, se entiende por:

a) Actuación administrativa automatizada: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

b) Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

c) Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

d) Autenticación: Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos, y de la integridad y autoría de estos últimos.

e) Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc).

f) Certificado electrónico: Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad».

g) Certificado electrónico reconocido: Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica: «Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten».

h) Ciudadano: Cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas.

i) Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

j) Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

k) Estándar abierto: Aquel que reúna las siguientes condiciones:

– sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

– su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

l) Firma electrónica: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante».

m) Firma electrónica avanzada: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control».

n) Firma electrónica reconocida: Según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma».

o) Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

p) Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

q) Punto de acceso electrónico: Conjunto de páginas web agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de a una institución pública.

r) Sistema de firma electrónica: Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

s) Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

t) Espacios comunes o ventanillas únicas: Modos o canales (oficinas integradas, atención telefónica, páginas en Internet y otros) a los que los ciudadanos pueden dirigirse para acceder a las informaciones, trámites y servicios públicos determinados por acuerdo entre varias Administraciones.

u) Actividad de servicio: Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.

v) Prestador de actividad de servicio: Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

§ 30

Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

Ministerio de la Presidencia
«BOE» núm. 278, de 18 de noviembre de 2009
Última modificación: 2 de octubre de 2015
Referencia: BOE-A-2009-18358

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, marca un hito trascendental en la construcción de la Administración pública de la sociedad de la información en España. Aunque apoyada en la experiencia adquirida con la aplicación de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común, en cuyos artículos 38, 45, 46 y 59, principalmente, ofrecía un marco jurídico general de referencia para la incorporación sistemática de las tecnologías de la información y de las comunicaciones a las funciones administrativas, así como en el avance que supuso la promulgación de la Ley 58/2003, de 17 de diciembre, General Tributaria, al recoger por primera vez la automatización de la actuación administrativa o la obtención de imágenes electrónicas de los documentos con idéntica validez y eficacia que el documento origen, lo cierto es que la Ley 11/2007, de 22 de junio, desborda el papel de solución de desarrollo o consolidación de la anterior por significar un verdadero replanteamiento de la relación entre la Administración y los ciudadanos.

La Ley 11/2007, de 22 de junio, impulsa una nueva concepción al construir su regulación sobre la base del derecho de los ciudadanos a utilizar los medios de comunicación electrónica para relacionarse con la Administración y ejercer sus derechos. Este singular punto de partida que pone al ciudadano y sus derechos en la base de todo, no sólo significa la imposición de un compromiso jurídico de incorporar las tecnologías de la información a la totalidad de las funciones administrativas. También, implica la consideración del ciudadano como portador de derechos de prestación que la Administración debe satisfacer de forma efectiva. Por ello, la ley estableció un elenco de derechos específicamente relacionados con la comunicación electrónica con la Administración y con su estatuto de ciudadano: derecho a la obtención de medios de identificación electrónica, derecho a elección del canal de comunicación o del medio de autentificación y de igualdad garantizando la accesibilidad, así como una efectiva igualdad entre géneros y respecto de otros colectivos con necesidades especiales y entre territorios.

Esta ambiciosa estrategia se ha asumido con una gran decisión. La disposición final tercera de la Ley 11/2007, de 22 de junio, establece la fecha del 31 de diciembre de 2009, como límite para que los ciudadanos puedan ejercer con plenitud sus derechos por medios electrónicos en cualquier procedimiento y actividad de competencia de dicha Administración.

El cumplimiento de los objetivos legales establecidos por la Ley 11/2007, de 22 de junio, y de los plazos previstos para su efectividad, justifican la necesidad de desarrollo de sus previsiones, en la medida que:

a) La Ley 11/2007, de 22 de junio, no agotó la regulación del acceso electrónico a los servicios públicos como consecuencia de los criterios de distribución de competencias y su incidencia en las competencias de autoorganización que corresponde al resto de las Administraciones públicas.

b) Por otro lado, por su carácter trasversal, esta regulación presupone operaciones de adaptación a los distintos procedimientos y actividades. El cumplimiento de esta necesidad solo puede lograrse mediante la previsión de un sistema de regulación caracterizado por la concurrencia de diferentes niveles normativos y la colaboración entre ellos para componer un marco general, objetivo, estable y predecible compatible con la adaptación funcional y con el estado del desarrollo tecnológico en esta materia.

El presente real decreto pretende ser ese complemento necesario en la Administración General del Estado para facilitar la efectiva realización de los derechos reconocidos en la Ley 11/2007, de 22 de junio.

Este real decreto se ha construido sobre la base de los siguientes principios estratégicos:

a) En primer lugar, procurar la más plena realización de los derechos reconocidos en la Ley 11/2007, de 22 de junio, facilitándolos en la medida que lo permite el estado de la técnica, y la garantía de que no resultan afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros.

b) En segundo lugar, establecer un marco lo más flexible posible en la implantación de los medios de comunicación, cuidando los niveles de seguridad y protección de derechos e intereses previstos tanto en la propia Ley 11/2007, de 22 de junio, como en la legislación administrativa en general. Con ello se persigue un triple objetivo: en primer lugar, evitar que la nueva regulación imponga una renovación tal en las soluciones de comunicación con los ciudadanos que impida la pervivencia de técnicas existentes y de gran arraigo; en segundo lugar, facilitar la actividad de implantación y adaptación a las distintas organizaciones, funciones y procedimientos a los que es de aplicación el real decreto; y en tercer lugar, impedir que la opción rígida por determinadas soluciones dificulte para el futuro la incorporación de nuevas soluciones y servicios.

No obstante, la realización de estos objetivos requiere de otros dos instrumentos de carácter técnico y complementario: el Esquema Nacional de Interoperabilidad, encargado de establecer los criterios comunes de gestión de la información que permitan compartir soluciones e información, y el Esquema Nacional de Seguridad que deberá establecer los criterios y niveles de seguridad necesarios para los procesos de tratamiento de la información que prevé el propio real decreto.

Fiel a esta orientación, el real decreto incorpora en su frontispicio una regulación específica destinada a hacer efectivo el derecho a no incorporar documentos que se encuentren en poder de las Administraciones públicas, estableciendo las reglas necesarias para obtener los datos y documentos exigidos, con las garantías suficientes que impidan que esta facilidad se convierta, en la práctica, en un motivo de retraso en la resolución de los procedimientos administrativos.

A estos efectos, se regula la forma y los efectos del ejercicio del derecho por parte de los ciudadanos, se contemplan los distintos supuestos que se pueden dar en cuanto a la obtención de los datos o documentos, se establecen plazos obligatorios para atender dichos requerimientos, así como el deber de informar sobre la demora en su cumplimiento para que el interesado pueda suplir la falta de actividad del órgano o entidad requerida, sin perjuicio de exigir las responsabilidades que, en su caso, procedan.

Un elemento clave en la comunicación jurídica con los ciudadanos en soporte electrónico es el concepto de sede electrónica. En este punto el real decreto pretende reforzar la fiabilidad de estos puntos de encuentro mediante tres tipos de medidas: 1) asegurar la plena identificación y diferenciación de estas direcciones como punto de prestación de servicios de comunicación con los interesados, 2) establecer el conjunto de servicios característicos así

como el alcance de su eficacia y responsabilidad, y 3) imponer un régimen común de creación de forma que se evite la desorientación que para el ciudadano podría significar una excesiva dispersión de tales direcciones. Este régimen de la sede, que debe resultar compatible con la descentralización necesaria derivada de la actual complejidad de fines y actividades asumidas por la Administración, resulta, sin embargo, compatible con la creación de un punto de acceso común a toda la Administración, puerta de entrada general del ciudadano a la Administración, en la que éste podrá presentar sus comunicaciones electrónicas generales o encontrar la información necesaria para acudir a las sedes electrónicas en las que iniciar o participar en los procedimientos que por ser tramitados en soporte electrónico, requieren el acceso a aplicaciones o formularios concretos.

En materia de identificación y autenticación el real decreto ha pretendido establecer los elementos mínimos imprescindibles para afianzar el criterio de flexibilización impulsado en la Ley 11/2007, de 22 de junio, en la que junto a la admisión como medio universal de los dispositivos de identificación y firma electrónica asociados al documento nacional de identidad, se admite la utilización de otros medios de autenticación que cumplan con las condiciones de seguridad y certeza necesarias para el normal desarrollo de la función administrativa.

Asimismo se ha previsto un régimen específico que facilita la actuación en nombre de terceros a través de dos mecanismos fundamentales: por un lado, la figura de las habilitaciones generales y especiales, pensadas fundamentalmente para el desempeño continuado y profesional de actividades de gestión y representación ante los servicios de la Administración, así como un registro voluntario de representantes, también pensado con la finalidad de facilitar el ejercicio de la función de representación, estableciendo un mecanismo de acreditación en línea del título previamente aportado a dicho registro.

El real decreto especifica igualmente las previsiones contenidas en la ley, en cuanto a la posibilidad de que los funcionarios públicos habilitados al efecto puedan realizar determinas operaciones por medios electrónicos usando sus propios sistemas de identificación y autenticación en aquellos casos en que los ciudadanos no dispongan de medios propios.

La relevancia jurídica de la actividad administrativa ha exigido prestar una atención singularizada al uso de los medios de identificación y autenticación electrónica por parte de la Administración, estableciendo la necesidad de incorporación de sellos o marcas de tiempo, que acrediten la fecha de adopción de los actos y documentos que se emitan. Igualmente se ha dispensado una atención especial a la autenticación en el seno de la actuación automatizada.

Por último se incorporan unas previsiones destinadas a garantizar la interoperabilidad y efectividad del sistema de la ley entre las que se incluye un reconocimiento expreso a las políticas de firma que serán los instrumentos encargados de especificar las soluciones técnicas y de organización necesarias para la plena operatividad de los derechos reconocidos en la ley, un sistema nacional de verificación de certificados dispuesto para simplificar y agilizar las operaciones de comprobación de la vigencia de los certificados.

En materia de registros electrónicos se han desarrollado las previsiones de la ley con la importante novedad de la creación de un registro electrónico común que posibilitará a los ciudadanos la presentación de comunicaciones electrónicas para cualquier procedimiento y órganos de los integrados en la Administración General del Estado y sus organismos públicos dependientes o vinculados.

Esta misma línea de desarrollo indispensable de las previsiones de la ley se ha seguido en relación con las comunicaciones y notificaciones electrónicas, estableciendo las garantías necesarias para que las facilidades incluidas en la Ley 11/2007, de 22 de junio, no se conviertan en una desventaja para los intereses de los ciudadanos así como del interés general.

Por último, uno de los puntos esenciales de la disciplina de la ley es la regulación de la gestión de la información electrónica aportada por los particulares, previéndose las condiciones mínimas para que su utilización no afecte al desarrollo de las funciones administrativas. Resulta especialmente innovadora la previsión en nuestro ordenamiento de un régimen de gestión y cambio de soporte con el fin de facilitar la gestión de los expedientes por la opción del órgano encargado de su tramitación del soporte tipo en el que deberá tramitarse el procedimiento. Igualmente el real decreto es consciente de la

importancia de integrar, desde la misma incorporación de los documentos, de aquella información que permita su gestión, archivo y recuperación. Asimismo, el real decreto, al regular los procesos de destrucción de documentos en papel que son objeto de copiado electrónico, establece un sistema reforzado de garantías con particular atención a la conservación de los documentos con valor histórico.

El presente real decreto se dicta en virtud de la habilitación expresa al Gobierno contenida en la disposición final séptima de la Ley 11/2007, de 22 de junio, y ha sido informado por la Agencia Española de Protección de Datos, el Consejo Superior de Administración Electrónica y el Consejo de Consumidores y Usuarios.

En su virtud, a propuesta de las Ministras de la Presidencia y de Economía y Hacienda y del Ministro de Industria, Turismo y Comercio, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros, en su reunión del día 6 de noviembre de 2009,

DISPONGO:

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto tiene por objeto desarrollar la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos en el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, en lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones y documentos electrónicos y copias.

2. Sus disposiciones son de aplicación:

a) A la actividad de la Administración General del Estado, así como de los organismos públicos vinculados o dependientes de la misma.

b) A los ciudadanos en sus relaciones con las entidades referidas en el párrafo anterior.

c) A las relaciones entre los órganos y organismos a los que se refiere el párrafo a).

Artículo 2. *Transmisiones de datos y documentos, incluidos certificados, entre órganos y organismos de la Administración General del Estado con ocasión del ejercicio reconocido por el artículo 6.2.b) de la Ley 11/2007, de 22 de junio.*

1. Cuando los ciudadanos ejerzan el derecho a no aportar datos y documentos que obren en poder de las Administraciones Públicas establecido en el artículo 6.2.b) de la Ley 11/2007, de 22 de junio, ante los órganos administrativos incluidos en el ámbito de aplicación del apartado 2.a) del artículo 1, de este real decreto, se seguirán las siguientes reglas:

a) La Administración facilitará a los interesados en los procedimientos administrativos el ejercicio del derecho, que podrá efectuarse por medios electrónicos.

En todo caso, los interesados serán informados expresamente de que el ejercicio del derecho implica su consentimiento, en los términos establecidos por el artículo 6. 2b) de la Ley 11/2007, de 22 de junio, para que el órgano y organismo ante el que se ejercita pueda recabar los datos o documentos respecto de los que se ejercita el derecho de los órganos u organismos en que los mismos se encuentren.

El derecho se ejercitará de forma específica e individualizada para cada procedimiento concreto, sin que el ejercicio del derecho ante un órgano u organismo implique un consentimiento general referido a todos los procedimientos que aquel tramite en relación con el interesado.

b) En cualquier momento, los interesados podrán aportar los datos o documentos o certificados necesarios, así como revocar su consentimiento para el acceso a datos de carácter personal.

c) Si el órgano administrativo encargado de la tramitación del procedimiento, posee, en cualquier tipo de soporte, los datos, documentos o certificados necesarios o tiene acceso electrónico a los mismos, los incorporará al procedimiento administrativo correspondiente sin más trámite. En todo caso, quedará constancia en los ficheros del órgano u organismo cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

d) Cuando el órgano administrativo encargado de la tramitación del procedimiento no tenga acceso a los datos, documentos o certificados necesarios, los pedirá al órgano administrativo correspondiente. Si se tratara de un órgano administrativo incluido en el ámbito de aplicación del artículo 1.2.a), deberá ceder por medios electrónicos los datos, documentos y certificados que sean necesarios en el plazo máximo que establezca la normativa específica, que no podrá exceder de diez días. Dicho plazo máximo será igualmente aplicable si no está fijado en la normativa específica.

e) En caso de imposibilidad de obtener los datos, documentos o certificados necesarios por el órgano administrativo encargado de la tramitación del procedimiento, se comunicará al interesado con indicación del motivo o causa, para que los aporte en el plazo y con los efectos previstos en la normativa reguladora del procedimiento correspondiente. En este caso, el interesado podrá formular queja conforme con lo previsto en el Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

f) Los órganos u organismos ante los que se ejercite el derecho conservarán la documentación acreditativa del efectivo ejercicio del derecho incorporándola al expediente en que el mismo se ejerció.

Dicha documentación estará a disposición del órgano cedente y de las autoridades a las que en su caso corresponda la supervisión y control de la legalidad de las cesiones producidas.

2. El Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad establecerán las previsiones necesarias para facilitar el ejercicio de este derecho por los ciudadanos.

Queda derogado el apartado 3 por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho apartado 3 se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"3. A fin de dar cumplimiento a la exigencia del artículo 9 de la Ley 11/2007, de 22 de junio, sobre transmisión de datos entre Administraciones Públicas, para un eficaz ejercicio del derecho reconocido en su artículo 6.2.b), la Administración General del Estado y sus organismos públicos promoverán la celebración de acuerdos o Convenios con las restantes Administraciones Públicas para facilitar el ejercicio de este derecho por los ciudadanos. En dichos acuerdos o Convenios se establecerán, en particular, los procedimientos que permitan al órgano u organismo cedente comprobar el efectivo ejercicio del derecho respecto de los datos o documentos cuyo acceso hubiera sido solicitado."

TÍTULO II

Sedes electrónicas y punto de acceso general a la Administración General del Estado

Artículo 3. *Creación de la sede electrónica.*

1. Los órganos de la Administración General del Estado y los organismos públicos vinculados o dependientes de la misma crearán sus sedes electrónicas, de acuerdo con los requisitos establecidos en el presente real decreto.

2. Las sedes electrónicas se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado», con el siguiente contenido mínimo:

a) Ámbito de aplicación de la sede, que podrá ser la totalidad del Ministerio u organismo público, o uno o varios de sus órganos con rango, al menos, de dirección general.

b) Identificación de la dirección electrónica de referencia de la sede.

c) Identificación de su titular, así como del órgano u órganos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos en la misma.

d) Identificación de los canales de acceso a los servicios disponibles en la sede, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.

e) Medios disponibles para la formulación de sugerencias y quejas.

f) Cualquier otra circunstancia que se considere conveniente para la correcta identificación de la sede y su fiabilidad.

3. También se podrán crear sedes compartidas mediante orden del Ministro de la Presidencia a propuesta de los Ministros interesados, cuando afecte a varios Departamentos ministeriales, o mediante convenio de colaboración cuando afecte a organismos públicos o cuando intervengan Administraciones autonómicas o locales, que deberá publicarse en el «Boletín Oficial del Estado». Los Convenios de colaboración podrán asimismo determinar la incorporación de un órgano u organismo a una sede preexistente.

Artículo 4. *Características de las sedes electrónicas.*

1. Se realizarán a través de sedes electrónicas todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración Pública o de los ciudadanos por medios electrónicos.

2. Se podrán crear una o varias sedes electrónicas derivadas de una sede electrónica. Las sedes electrónicas derivadas, o subsedes, deberán resultar accesibles desde la dirección electrónica de la sede principal, sin perjuicio de que sea posible el acceso electrónico directo.

Las sedes electrónicas derivadas deberán cumplir los mismos requisitos que las sedes electrónicas principales, salvo en lo relativo a la publicación de la orden o resolución por la que se crea, que se realizará a través de la sede de la que dependan. Su ámbito de aplicación comprenderá órgano u órganos con rango, al menos, de subdirección general.

Artículo 5. *Condiciones de identificación de las sedes electrónicas y seguridad de sus comunicaciones.*

1. Las direcciones electrónicas de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma que tengan la condición de sedes electrónicas deberán hacerlo constar de forma visible e inequívoca.

2. La sede electrónica tendrá accesible su instrumento de creación, directamente o mediante enlace a su publicación en el «Boletín Oficial del Estado».

3. Las condiciones de identificación de las sedes electrónicas y de seguridad de sus comunicaciones se regirán por lo dispuesto en el título tercero del presente real decreto, y en

el título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

4. Los sistemas de información que soporten las sedes electrónicas deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. El Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad establecerán las previsiones necesarias para ello.

Artículo 6. *Contenido y servicios de las sedes electrónicas.*

1. Toda sede electrónica dispondrá del siguiente contenido mínimo:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión y de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para la correcta utilización de la sede incluyendo el mapa de la sede electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relacionada con propiedad intelectual.

c) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

d) Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

e) Relación de sistemas de firma electrónica que, conforme a lo previsto en este real decreto, sean admitidos o utilizados en la sede.

f) **(Derogada)**

Téngase en cuenta que la letra f) del apartado 1 queda derogada por la disposición derogatoria única.g) de la Ley 40/2015, de 1 de octubre. Ref. BOE-A-2015-10566. a partir del 2 de octubre de 2016, según establece su disposición final. 18.1

Redacción anterior:
"f) Normas de creación del registro o registros electrónicos accesibles desde la sede."

g) Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos.

2. Las sedes electrónicas dispondrán de los siguientes servicios a disposición de los ciudadanos:

a) Relación de los servicios disponibles en la sede electrónica.

b) Carta de servicios y carta de servicios electrónicos.

c) Relación de los medios electrónicos a los que se refiere el artículo 27.4 de la Ley 11/2007, de 22 de junio.

d) Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

e) Acceso, en su caso, al estado de tramitación del expediente.

f) En su caso, publicación de los diarios o boletines.

g) En su caso, publicación electrónica de actos y comunicaciones que deban publicarse en tablón de anuncios o edictos, indicando el carácter sustitutivo o complementario de la publicación electrónica.

h) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

i) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

j) Indicación de la fecha y hora oficial a los efectos previstos en el artículo 26.1 de la Ley 11/2007, de 22 de junio.

3. Los órganos titulares responsables de la sede podrán además incluir en la misma otros servicios o contenidos, con sujeción a lo previsto en el artículo 10 de la Ley 11/2007, de 22 de junio, y en este real decreto.

4. No será necesario recoger en las subsedes la información y los servicios a que se refieren los apartados anteriores cuando ya figuren en la sede de la que aquéllas derivan.

5. Las sedes electrónicas cuyo titular tenga competencia sobre territorios con régimen de cooficialidad lingüística posibilitarán el acceso a sus contenidos y servicios en las lenguas correspondientes.

Artículo 7. *Reglas especiales de responsabilidad.*

1. El establecimiento de una sede electrónica conllevará la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma. El titular de la sede electrónica que contenga un enlace o vínculo a otra cuya responsabilidad corresponda a distinto órgano o Administración Pública no será responsable de la integridad, veracidad ni actualización de esta última.

La sede establecerá los medios necesarios para que el ciudadano conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero.

2. Los órganos u organismos públicos titulares de las sedes electrónicas compartidas previstas en el artículo 3.3 del presente real decreto, responderán, en todo caso, por sus contenidos propios y solidariamente por los contenidos comunes.

Artículo 8. *Directorio de sedes electrónicas.*

1. El Ministerio de la Presidencia gestionará un directorio de sedes electrónicas de la Administración General del Estado y de sus organismos públicos, que será público y accesible desde el punto de acceso general al que se refiere el artículo 9 de este real decreto.

2. En dicho directorio se publicarán las sedes con expresión de su denominación, ámbito de aplicación, titular y la dirección electrónica de las mismas.

Artículo 9. *Punto de acceso general de la Administración General del Estado.*

1. El Punto de acceso general de la Administración General del Estado contendrá la sede electrónica que, en este ámbito, facilita el acceso a los servicios, procedimientos e informaciones accesibles de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras Administraciones públicas, mediante la celebración de los correspondientes Convenios.

2. El acceso se organizará atendiendo a distintos criterios que permitan a los ciudadanos identificar de forma fácil e intuitiva los servicios a los que deseen acceder.

3. El Punto de acceso general será gestionado por el Ministerio de la Presidencia, con la participación de todos los Ministerios y, en su caso, de los organismos públicos dotados por la ley de un régimen especial de independencia, para garantizar la completa y exacta incorporación de la información y accesos publicados en éste.

4. El Punto de acceso general podrá incluir servicios adicionales, así como distribuir la información sobre el acceso electrónico a los servicios públicos de manera que pueda ser utilizada por otros departamentos ministeriales, Administraciones o por el sector privado.

TÍTULO III

Identificación y autenticación

CAPÍTULO I

Identificación y autenticación en el acceso electrónico de los ciudadanos a la Administración General del Estado y sus organismos públicos vinculados o dependientes

Artículo 10. *Firma electrónica de los ciudadanos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 10. Firma electrónica de los ciudadanos.**
1. Las personas físicas podrán utilizar para relacionarse electrónicamente con la Administración General del Estado y los organismos públicos vinculados o dependientes, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, en todo caso, y los sistemas de firma electrónica avanzada admitidos, a los que se refiere el artículo 13.2.b) de la Ley 11/2007, de 22 de junio.
2. Las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica de persona jurídica o de entidades sin personalidad jurídica para todos aquellos procedimientos y actuaciones de la Administración General del Estado para los que se admitan.
3. En caso de no admisión, la sede electrónica correspondiente deberá facilitar sistemas alternativos que permitan a las personas jurídicas y a las entidades sin personalidad jurídica el ejercicio de su derecho a relacionarse electrónicamente con la Administración General del Estado."

Artículo 11. *Otros sistemas de firma electrónica.*

1. La admisión de otros sistemas de firma electrónica a la que se refiere el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberán aprobarse mediante orden ministerial, o resolución del titular en el caso de los organismos públicos, previo informe del Consejo Superior de Administración Electrónica.

2. Cuando el sistema se refiera a la totalidad de la Administración General del Estado, se requerirá acuerdo del Consejo de Ministros a propuesta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

3. El acto de aprobación contendrá la denominación y descripción general del sistema de identificación, órgano u organismo público responsable de su aplicación y garantías de su funcionamiento, y será publicado en las sedes electrónicas que sean de aplicación, donde se informará de las actuaciones en las que son admisibles estos medios de identificación y autenticación.

Artículo 12. *Disposiciones comunes al régimen de uso de la firma electrónica.*

1. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación que le sea aplicable.

2. El uso por los ciudadanos de sistemas de firma electrónica implicará que los órganos de la Administración General del Estado u organismos públicos vinculados o dependientes pueden tratar los datos personales consignados, a los efectos de la verificación de la firma.

Artículo 13. *Habilitación para la representación de terceros.*

(Derogado).

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 13. Habilitación para la representación de terceros.**
1. De acuerdo con lo previsto en el artículo 23 de la Ley 11/2007, de 22 de junio, la Administración General del Estado y sus organismos públicos vinculados o dependientes podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la presentación electrónica de documentos en representación de los interesados.
La habilitación conllevará la aplicación del régimen de representación regulado en el artículo siguiente.
2. La habilitación requerirá la firma previa de un convenio entre el Ministerio u organismo público competente y la corporación, asociación o institución interesada. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la persona jurídica o entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas.
Se determinará en cada caso, mediante orden ministerial del Departamento titular de la gestión, los requisitos y condiciones para suscribir los Convenios a que se refiere el presente apartado. Dicha orden deberá garantizar en todo caso el respeto a los principios de objetividad, proporcionalidad y no discriminación en la definición de las condiciones para la habilitación.
3. Los Convenios de habilitación surtirán efectos tanto en relación con la corporación, asociación o institución firmante como con las personas, físicas o jurídicas, que tengan la condición de colegiados, asociados o miembros de aquéllas. Para hacer efectiva la habilitación, éstas últimas deberán suscribir un documento individualizado de adhesión que recoja expresamente la aceptación de su contenido íntegro.
4. El incumplimiento de las obligaciones asumidas por las corporaciones, asociaciones o instituciones firmantes del convenio supondrá su resolución y la de las habilitaciones basadas en el mismo, previa instrucción del oportuno expediente, con audiencia de la entidad interesada.
El incumplimiento por parte de una persona firmante del documento individualizado de adhesión supondrá su exclusión del convenio con el procedimiento y garantías previstos en el párrafo anterior.
En ambos casos se entenderá sin perjuicio de la exigencia de las responsabilidades que fueran procedentes."

Artículo 14. *Régimen de la representación habilitada ante la Administración.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 14. Régimen de la representación habilitada ante la Administración.**

1. Las personas o entidades habilitadas para la presentación electrónica de documentos en representación de terceros deberán ostentar la representación necesaria para cada actuación, en los términos establecidos en el artículo 32 de la Ley 30/1992, de 26 de noviembre, o en los términos que resulten de la normativa específica de aplicación.
2. La Administración podrá requerir en cualquier momento a las personas habilitadas la acreditación de la representación que ostenten, siendo válida la otorgada a través de los documentos normalizados que apruebe la Administración para cada procedimiento.
La falta de representación suficiente de las personas en cuyo nombre se hubiera presentado la documentación dará lugar a la exigencia de las responsabilidades que fueran procedentes.
3. La habilitación sólo confiere a la persona autorizada la condición de representante para intervenir en los actos expresamente autorizados. No autoriza a recibir ninguna comunicación de la Administración en nombre del interesado, aun cuando éstas fueran consecuencia del documento presentado.
4. La representación habilitada sólo permite la presentación de solicitudes, escritos o comunicaciones en los registros electrónicos correspondientes al ámbito de la habilitación."

Artículo 15. *Registro electrónico de apoderamientos para actuar ante la Administración General del Estado y sus organismos públicos vinculados o dependientes.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 15. Registro electrónico de apoderamientos para actuar ante la Administración General del Estado y sus organismos públicos vinculados o dependientes.**
1. A los efectos de la actuación administrativa ante la Administración General del Estado y sus organismos públicos vinculados o dependientes y sin carácter de registro público, se crea, en su ámbito, el registro electrónico de apoderamientos. En él se podrán hacer constar todas las representaciones que los interesados otorguen a terceros para actuar en su nombre ante la Administración General del Estado y sus organismos públicos vinculados o dependientes.
2. El Ministerio de la Presidencia creará los ficheros de datos personales necesarios y gestionará dicho registro, que deberá coordinarse con cualquier otro similar existente de ámbito más limitado en la Administración General del Estado.
3. El registro de apoderamientos permitirá a los Ministerios y a los organismos públicos vinculados o dependientes de la Administración General del Estado que se suscriban al mismo, comprobar la representación que ostentan quienes actúen electrónicamente ante ellos en nombre de terceros.
4. Cada Departamento Ministerial y organismo público determinará los trámites y actuaciones de su competencia para los que sea válida la representación incorporada al registro de apoderamientos. Además, caso de entender que hay falta o insuficiencia de la representación formalmente incorporada al registro de apoderamientos podrá requerir al interesado la correspondiente subsanación en los términos del artículo 32.4 de la Ley 30/1992, de 26 de noviembre, o en los términos que resulten de la normativa específica de aplicación.
5. A efectos de su incorporación al registro electrónico de apoderamientos y demás aspectos relativos a su funcionamiento, mediante orden del Ministro de la Presidencia se concretará el régimen de otorgamiento de los apoderamientos, sus formas de acreditación, ámbito de aplicación y revocación de los poderes, así como la forma y lugar de presentación de los documentos acreditativos del poder."

Artículo 16. *Identificación y autenticación de los ciudadanos por funcionario público.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 16. Identificación y autenticación de los ciudadanos por funcionario público.**
1. Para llevar a cabo la identificación y autenticación de los ciudadanos por funcionario público conforme a lo previsto en el artículo 22 de la Ley 11/2007, de 22 de junio, en los servicios y procedimientos para los que así se establezca, y en los que resulte necesaria la utilización de sistemas de firma electrónica de los que aquéllos carezcan, se requerirá que el funcionario público habilitado esté dotado de un sistema de firma electrónica admitido por el órgano u organismo público destinatario de la actuación para la que se ha de realizar la identificación o autenticación. El ciudadano, por su parte, habrá de identificarse ante el funcionario y prestar consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.
2. El Ministerio de la Presidencia mantendrá actualizado un registro de los funcionarios habilitados en la Administración General del Estado y sus organismos públicos para la identificación y autenticación regulada en este artículo. Mediante el correspondiente Convenio de colaboración podrá extender sus efectos a las relaciones con otras Administraciones públicas.
3. Mediante orden del Ministro de la Presidencia se regulará el funcionamiento del registro de funcionarios habilitados, incluido el sistema para la determinación de los funcionarios que puedan ser habilitados y el alcance de la habilitación.
4. Adicionalmente, los Departamentos Ministeriales y organismos públicos podrán habilitar funcionarios públicos en ellos destinados para identificar y autenticar a ciudadanos ante dicho Departamento ministerial u organismo público."

CAPÍTULO II

Identificación y autenticación de sedes electrónicas y de las comunicaciones que realicen los órganos de la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla

Artículo 17. *Identificación de sedes electrónicas de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.*

1. Las sedes electrónicas se identificarán mediante sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente. Con carácter adicional y para su identificación inmediata, los ciudadanos dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en el presente real decreto.

2. Para facilitar su identificación, las sedes electrónicas seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio de tercer nivel «.gob.es».

Artículo 18. *Certificados de sede electrónica de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.*

1. Los certificados electrónicos de sede electrónica tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sede electrónica».
b) Nombre descriptivo de la sede electrónica.
c) Denominación del nombre del dominio.
d) Número de identificación fiscal de la entidad suscriptora.
e) Unidad administrativa suscriptora del certificado.

2. El uso de los certificados de sede electrónica está limitado a la identificación de la sede, quedando excluida su aplicación para la firma electrónica de documentos y trámites.

3. El Esquema Nacional de Seguridad, al que se refiere el artículo 42 de la Ley 11/2007, de 22 de junio, determinará las características y requisitos que cumplirán los sistemas de firma electrónica, los certificados y los medios equivalentes que se establezcan en las sedes electrónicas para la identificación y garantía de una comunicación segura.

Artículo 19. *Sistemas de firma electrónica mediante sello electrónico.*

1. La creación de sellos electrónicos se realizará mediante resolución de la Subsecretaría del Ministerio o titular del organismo público competente, que se publicará en la sede electrónica correspondiente y en la que deberá constar:

a) Organismo u órgano titular del sello que será el responsable de su utilización, con indicación de su adscripción en la Administración General del Estado u organismo público dependiente de la misma.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado.

2. Los certificados de sello electrónico tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».

b) Nombre del suscriptor.

c) Número de identificación fiscal del suscriptor.

3. El modo de emitir los certificados electrónicos de sello electrónico se definirá en el Esquema Nacional de Seguridad.

Artículo 20. *Sistemas de código seguro de verificación.*

1. La Administración General del Estado y sus organismos públicos vinculados o dependientes podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas. Dicho código vinculará al órgano u organismo y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El carácter único del código generado para cada documento.

b) Su vinculación con el documento generado y con el firmante.

c) Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

3. La aplicación de este sistema requerirá una orden del Ministro competente o resolución del titular del organismo público, previo informe del Consejo Superior de Administración Electrónica, que se publicará en la sede electrónica correspondiente. Dicha orden o resolución del titular del organismo público, además de describir el funcionamiento del sistema, deberá contener de forma inequívoca:

a) Actuaciones automatizadas a las que es de aplicación el sistema.

b) Órganos responsables de la aplicación del sistema.

c) Disposiciones que resultan de aplicación a la actuación.

d) Indicación de los mecanismos utilizados para la generación del código.

e) Sede electrónica a la que pueden acceder los interesados para la verificación del contenido de la actuación o documento.

f) Plazo de disponibilidad del sistema de verificación respecto a los documentos autorizados mediante este sistema.

4. La Administración responsable de la aplicación de este sistema dispondrá de un procedimiento directo y gratuito para los interesados. El acceso a los documentos originales se realizará de acuerdo con las condiciones y límites que establece la legislación de protección de datos personales u otra legislación específica, así como el régimen general de

acceso a la información administrativa establecido en el artículo 37 de la Ley 30/1992, de 26 de noviembre.

5. Se adoptarán las medidas necesarias para garantizar la constancia de la autenticación e integridad de los documentos con posterioridad al vencimiento del plazo de disponibilidad del sistema de verificación, a los efectos de su posterior archivo.

6. Con el fin de mejorar la interoperabilidad electrónica y posibilitar la verificación de la autenticidad de los documentos electrónicos sin necesidad de acceder a la sede electrónica para cotejar el código seguro de verificación, podrá superponerse a éste la firma mediante sello electrónico regulada en el artículo anterior.

Artículo 21. *Firma electrónica mediante medios de autenticación personal.*

El personal al servicio de la Administración General del Estado y de sus organismos públicos vinculados o dependientes utilizará los sistemas de firma electrónica que se determinen en cada caso, entre los siguientes:

a) Firma basada en el Documento Nacional de Identidad electrónico.

b) Firma basada en certificado de empleado público al servicio de la Administración General del Estado expresamente admitidos con esta finalidad.

c) Sistemas de código seguro de verificación, en cuyo caso se aplicará, con las adaptaciones correspondientes, lo dispuesto en el artículo 20.

Artículo 22. *Características de los sistemas de firma electrónica basados en certificados facilitados al personal de la Administración General del Estado o de sus organismos públicos.*

1. Los sistemas de firma electrónica basados en certificados facilitados específicamente a sus empleados por la Administración General del Estado o sus organismos públicos vinculados o dependientes sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan.

2. La firma electrónica regulada en el presente artículo deberá cumplir con las garantías que se establezcan en las políticas de firma que sean aplicables.

3. Los certificados emitidos para la firma, se denominarán «certificado electrónico de empleado público» y tendrán, al menos, el siguiente contenido:

a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público».

b) Nombre y apellidos del titular del certificado.

c) Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado.

d) Órgano u organismo público en el que presta servicios el titular del certificado.

e) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

4. Los contenidos especificados en el apartado anterior no serán exigibles para los certificados que se utilicen en aquellas actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización. En estos casos, los prestadores de servicios de certificación podrán consignar en el certificado electrónico, a petición de la Administración solicitante, un seudónimo. Estos certificados se denominarán certificados electrónicos de empleado público con seudónimo. Tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público y al menos, el siguiente contenido:

a) Descripción del tipo de certificado en el que deberá incluirse la denominación "certificado electrónico de empleado público con seudónimo".

b) Seudónimo del titular del certificado, consistente en su número de identificación profesional u otro indicador proporcionado por la Administración correspondiente.

c) Órgano u organismo público en el que presta servicios el titular del certificado.

d) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado.

Los órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado electrónico de empleado público con seudónimo, en los casos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En ese caso, el prestador de servicios de certificación actuará de conformidad con lo previsto en la Ley 59/2003, de 19 de diciembre.

CAPÍTULO III

Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad

Artículo 23. *Obligaciones de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación admitidos deberán cumplir las obligaciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como las condiciones generales adicionales a que se refiere el apartado 3.

2. Los prestadores de servicios de certificación deberán facilitar a las plataformas públicas de validación que se establezcan conforme a lo previsto en este real decreto, acceso electrónico y gratuito para la verificación de la vigencia de los certificados asociados a sistemas utilizados por los ciudadanos, la Administración General del Estado y sus organismos públicos.

3. Las condiciones generales adicionales a que se refiere el artículo 4.3 de la Ley 59/2003, de 19 de diciembre, se aprobarán mediante real decreto aprobado por el Consejo de Ministros a propuesta conjunta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

Corresponde a los Ministerios de la Presidencia y de Industria, Turismo y Comercio publicar la relación de prestadores de servicios de certificación admitidos y de controlar el cumplimiento de las condiciones generales adicionales que se establezcan.

Artículo 24. *Política de firma electrónica y de certificados.*

1. La política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

2. Sin perjuicio de lo dispuesto en el artículo 23, la política de firma electrónica y certificados deberá contener en todo caso:

a) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos.

b) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de certificación asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado recogidas en el presente real decreto.

c) La definición de su ámbito de aplicación.

3. La política de firma electrónica y certificados será aprobada por el Consejo Superior de Administración Electrónica. Mediante resolución del Secretario de Estado para la Función Pública se publicará en el «Boletín Oficial del Estado» el acuerdo de aprobación de la política de firma electrónica y certificados extractado, y de forma íntegra en la sede del Punto de acceso general de la Administración General del Estado.

Artículo 25. *Plataformas de verificación de certificados y sistema nacional de verificación.*

1. El Ministerio de la Presidencia gestionará una plataforma de verificación del estado de revocación de los certificados admitidos en el ámbito de la Administración General del Estado y de los organismos públicos dependientes o vinculados a ella, de acuerdo con lo previsto en el artículo 21.3 de la Ley 11/2007, de 22 de junio. Esta plataforma permitirá

verificar el estado de revocación y el contenido de los certificados y prestará el servicio de forma libre y gratuita a todas las Administraciones públicas, españolas o europeas.

2. En el ámbito de sus competencias, los departamentos ministeriales y organismos públicos podrán disponer de sus propias plataformas de verificación del estado de revocación de los certificados.

3. Para mejorar la calidad, robustez y disponibilidad de los servicios de verificación que se ofrecen a todas las Administraciones públicas, se creará el sistema nacional de verificación de certificados compuesto por la Plataforma referida en el apartado uno y aquellas otras que, cumpliendo con lo especificado en el apartado cuatro, se adhieran al mismo. Las plataformas adheridas al sistema nacional podrán delegar operaciones concretas de verificación en cualquiera de ellas. En particular, la operada por el Ministerio de la Presidencia proporcionará servicios de validación de certificados del ámbito europeo al resto de plataformas.

4. Las plataformas de servicios de validación que se integren en el sistema nacional de verificación de certificados deberán cumplir con los siguientes requisitos:

a) Deberán poder obtener y procesar de forma automática las listas de certificados admitidos expedidas de acuerdo con lo establecido en este real decreto y cumplirán con las particularidades que se establezcan en la política de firma y certificados electrónicos que sea de aplicación.

b) Deberán resultar accesibles y prestar sus servicios prioritariamente a través de la red de comunicaciones de las Administraciones Públicas españolas, en las condiciones de seguridad y disponibilidad adecuadas al volumen y la criticidad de los servicios que las usen, pudiendo no obstante contar, como respaldo, con otras vías de acceso.

c) Deberán disponer de documentación y procedimientos operativos del servicio.

d) Deberán garantizar un nivel de servicio que asegure la disponibilidad de la información de estado y validación de certificados en las condiciones que se establezcan en la política de firma y certificados electrónicos.

e) Dispondrán de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir en relación con los servicios de verificación. La declaración estará disponible al público por vía electrónica y con carácter gratuito.

f) Deberán habilitar los mecanismos y protocolos de llamada y de sincronización que sean necesarios para crear el sistema nacional de verificación de certificados y acceder a los servicios universales de validación que ofrezca la plataforma operada por el Ministerio de la Presidencia. Basarán su operatividad en las directrices definidas en la política de firma y certificados electrónicos en el ámbito de la Administración General del Estado.

g) Cumplirán lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad respecto de las condiciones generales a las que deberán someterse las plataformas y servicios de validación de certificados.

TÍTULO IV

Registros electrónicos

Artículo 26. *Registros electrónicos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 26. Registros electrónicos.**

Todos los Departamentos Ministeriales de la Administración General del Estado, así como sus organismos públicos, deberán disponer de un servicio de registro electrónico, propio o proporcionado por otro órgano u organismo, para la recepción y remisión de solicitudes, escritos y comunicaciones correspondientes a los procedimientos y actuaciones de su competencia."

Artículo 27. *Creación de registros electrónicos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 27. Creación de registros electrónicos.**
1. La creación de registros electrónicos se efectuará mediante orden del Ministro respectivo o resolución del titular del organismo público, previa aprobación del Ministro de la Presidencia salvo para los organismos públicos en los que no resulte preceptiva, de acuerdo con su normativa específica de organización. Los organismos públicos podrán utilizar los registros electrónicos del departamento ministerial del que dependan, para lo cual suscribirán el correspondiente Convenio.
2. Las disposiciones que creen registros electrónicos contendrán, al menos:

a) Órgano o unidad responsable de la gestión.
b) Fecha y hora oficial y referencia al calendario de días inhábiles que sea aplicable.
c) Identificación del órgano u órganos competentes para la aprobación y modificación de la relación de documentos electrónicos normalizados, que sean del ámbito de competencia del registro, e identificación de los trámites y procedimientos a que se refieren.
d) Medios de presentación de documentación complementaria a una comunicación, escrito o solicitud previamente presentada en el registro electrónico.

3. En ningún caso tendrán la condición de registro electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas unidades y órganos.
4. Tampoco tendrán la consideración de registro electrónico los dispositivos de recepción de fax, salvo aquellos supuestos expresamente previstos en el ordenamiento jurídico."

Artículo 28. *Funciones de los registros electrónicos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 28. Funciones de los registros electrónicos.**
Los registros electrónicos realizarán las siguientes funciones:

a) La recepción y remisión de solicitudes, escritos y comunicaciones relativas a los trámites y procedimientos que correspondan de acuerdo con su norma de creación, y de los documentos adjuntos, así como la emisión de los recibos necesarios para confirmar la recepción en los términos previstos en el artículo 25 de la Ley 11/2007, de 22 de junio.

b) La remisión electrónica de escritos, solicitudes y comunicaciones a las personas, órganos o unidades destinatarias en los términos del presente real decreto y del artículo 24.2.b) de la Ley 11/2007, de 22 de junio.
c) La anotación de los correspondientes asientos de entrada y salida.
d) Funciones de constancia y certificación en los supuestos de litigios, discrepancias o dudas acerca de la recepción o remisión de solicitudes, escritos y comunicaciones."

Artículo 29. *Solicitudes, escritos y comunicaciones que pueden ser rechazados en los registros electrónicos.*

1. Los registros electrónicos podrán rechazar los documentos electrónicos que se les presenten, en las siguientes circunstancias:

a) **(Derogada)**

Queda derogada la letra a) del apartado 1 por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicha letra a) se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"a) Que se trate de documentos dirigidos a órganos u organismos fuera del ámbito de la Administración General del Estado."

b) Que contengan código malicioso o dispositivo susceptible de afectar a la integridad o seguridad del sistema.

c) En el caso de utilización de documentos normalizados, cuando no se cumplimenten los campos requeridos como obligatorios en la resolución de aprobación del correspondiente documento, o cuando contenga incongruencias u omisiones que impidan su tratamiento.

d) **(Derogada)**

Queda derogada la letra d) del apartado 1 por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicha letra d), se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"d) Que se trate de documentos que de acuerdo con lo establecido en los artículos 14 y 32 deban presentarse en registros electrónicos específicos."

2. En los casos previstos en el apartado anterior, se informará de ello al remitente del documento, con indicación de los motivos del rechazo así como, cuando ello fuera posible, de los medios de subsanación de tales deficiencias y dirección en la que pueda presentarse. Cuando el interesado lo solicite se remitirá justificación del intento de presentación, que incluirá las circunstancias de su rechazo.

3. Cuando concurriendo las circunstancias previstas en el apartado 1, no se haya producido el rechazo automático por el registro electrónico, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiendo que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia.

Artículo 30. *Recepción de solicitudes, escritos y comunicaciones.*

1. La presentación de solicitudes, escritos y comunicaciones podrá realizarse en los registros electrónicos durante las veinticuatro horas de todos los días del año.

2. La recepción de solicitudes, escritos y comunicaciones podrá interrumpirse por el tiempo imprescindible sólo cuando concurran razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios del registro electrónico con la antelación que, en cada caso, resulte posible.

En supuestos de interrupción no planificada en el funcionamiento del registro electrónico, y siempre que sea posible, se dispondrán las medidas para que el usuario resulte informado de esta circunstancia así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. Alternativamente, podrá establecerse un redireccionamiento que permita utilizar un registro electrónico en sustitución de aquél en el que se haya producido la interrupción.

3. El registro electrónico emitirá automáticamente por el mismo medio un recibo firmado electrónicamente, mediante alguno de los sistemas de firma del artículo 18 de la Ley 11/2007, de 22 de junio, con el siguiente contenido:

a) Copia del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.

b) Fecha y hora de presentación y número de entrada de registro.

c) En su caso, enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.

d) Información del plazo máximo establecido normativamente para la resolución y notificación del procedimiento, así como de los efectos que pueda producir el silencio administrativo, cuando sea automáticamente determinable.

Artículo 31. *Creación, naturaleza y funcionamiento del Registro Electrónico Común.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:

"**Artículo 31. Creación, naturaleza y funcionamiento del Registro Electrónico Común.**

1. Se crea el Registro Electrónico Común de la Administración General del Estado, accesible a través del punto de acceso general establecido en el artículo 9.

2. El Registro Electrónico Común será gestionado por el Ministerio de la Presidencia.

3. El Registro Electrónico Común posibilitará la presentación de cualesquiera solicitudes, escritos y comunicaciones dirigidas a la Administración General del Estado y a sus organismos públicos.

4. El Registro Electrónico Común informará al ciudadano y le redirigirá, cuando proceda, a los registros competentes para la recepción de aquellos documentos que dispongan de aplicaciones específicas para su tratamiento.

5. Mediante orden del Ministro de la Presidencia se establecerán los requisitos y condiciones de funcionamiento del Registro Electrónico Común, incluyendo la creación de un fichero ajustado a las previsiones de la normativa sobre protección de datos de carácter personal, así como los demás aspectos previstos en el artículo 27.2."

TÍTULO V

De las comunicaciones y las notificaciones

CAPÍTULO I

Comunicaciones electrónicas

Artículo 32. *Obligatoriedad de la comunicación a través de medios electrónicos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 32. Obligatoriedad de la comunicación a través de medios electrónicos.**
1. La obligatoriedad de comunicarse por medios electrónicos con los órganos de la Administración General del Estado o sus organismos públicos vinculados o dependientes, en los supuestos previstos en el artículo 27.6 de la Ley 11/2007, de 22 de junio, podrá establecerse mediante orden ministerial. Esta obligación puede comprender, en su caso, la práctica de notificaciones administrativas por medios electrónicos, así como la necesaria utilización de los registros electrónicos que se especifiquen.
2. En la norma que establezca dicha obligación se especificarán las comunicaciones a las que se aplique, el medio electrónico de que se trate y los sujetos obligados. Dicha orden deberá ser publicada en el «Boletín Oficial del Estado» y en la sede electrónica del órgano u organismo público de que se trate.
3. Si existe la obligación de comunicación a través de medios electrónicos y no se utilizan dichos medios, el órgano administrativo competente requerirá la correspondiente subsanación, advirtiendo que, de no ser atendido el requerimiento, la presentación carecerá de validez o eficacia."

Artículo 33. *Modificación del medio de comunicación inicialmente elegido.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 33. Modificación del medio de comunicación inicialmente elegido.**
Salvo las excepciones previstas en el artículo anterior, los ciudadanos podrán modificar la manera de comunicarse con los órganos u organismos públicos vinculados o dependientes de la Administración General del Estado, optando por un medio distinto del inicialmente elegido, que comenzará a producir efectos respecto de las comunicaciones que se produzcan a partir del día siguiente a su recepción en el registro del órgano competente."

Artículo 34. *Comunicaciones entre los órganos de la Administración General del Estado y sus organismos públicos.*

1. Los órganos de la Administración General del Estado y sus organismos públicos deberán utilizar medios electrónicos para comunicarse entre ellos. Sólo con carácter excepcional se podrán utilizar otros medios de comunicación cuando no sea posible la utilización de medios electrónicos por causas justificadas de carácter técnico.

2. Los órganos de la Administración General del Estado y sus organismos públicos deberán utilizar medios electrónicos para comunicarse con otras Administraciones públicas. No obstante, se podrán utilizar otros medios de comunicación atendiendo a los medios técnicos de que éstas dispongan.

Se suscribirán los Convenios necesarios para garantizar las condiciones de dicha comunicación, salvo cuando dichas condiciones se encuentren reguladas en normas específicas.

CAPÍTULO II

Notificaciones electrónicas

Artículo 35. *Práctica de notificaciones por medios electrónicos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 35. Práctica de notificaciones por medios electrónicos.**
1. Los órganos y organismos públicos de la Administración General del Estado habilitarán sistemas de notificación electrónica de acuerdo con lo dispuesto en el presente capítulo.
2. La práctica de notificaciones por medios electrónicos podrá efectuarse, de alguna de las formas siguientes:

a) Mediante la dirección electrónica habilitada en la forma regulada en el artículo 38 de este real decreto.
b) Mediante sistemas de correo electrónico con acuse de recibo que deje constancia de la recepción en la forma regulada en el artículo 39 de este real decreto.
c) Mediante comparecencia electrónica en la sede en la forma regulada en el artículo 40 de este real decreto.
d) Otros medios de notificación electrónica que puedan establecerse, siempre que quede constancia de la recepción por el interesado en el plazo y en las condiciones que se establezcan en su regulación específica."

Artículo 36. *Elección del medio de notificación.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 36. Elección del medio de notificación.**
1. Las notificaciones se efectuarán por medios electrónicos cuando así haya sido solicitado o consentido expresamente por el interesado o cuando haya sido establecida como obligatoria conforme a lo dispuesto en los artículos 27.6 y 28.1 de la Ley 11/2007, de 22 de junio.
2. La solicitud deberá manifestar la voluntad de recibir las notificaciones por alguna de las formas electrónicas reconocidas, e indicar un medio de notificación electrónica válido conforme a lo establecido en el presente real decreto.
3. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento podrán emitirse y recabarse, en todo caso, por medios electrónicos.
4. Cuando la notificación deba admitirse obligatoriamente por medios electrónicos, el interesado podrá elegir entre las distintas formas disponibles salvo que la normativa que establece la notificación electrónica obligatoria señale una forma específica.
5. Cuando, como consecuencia de la utilización de distintos medios, electrónicos o no electrónicos, se practiquen varias notificaciones de un mismo acto administrativo, se entenderán producidos todos los efectos jurídicos derivados de la notificación, incluido el inicio del plazo para la interposición de los recursos que procedan, a partir de la primera de las notificaciones correctamente practicada. Las Administraciones públicas podrán advertirlo de este modo en el contenido de la propia notificación.
6. Se entenderá consentida la práctica de la notificación por medios electrónicos respecto de una determinada actuación administrativa cuando, tras haber sido realizada por una de las formas válidamente reconocidas para ello, el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación. La notificación surtirá efecto a partir de la fecha en que el interesado realice dichas actuaciones.
En el supuesto previsto en el párrafo anterior, el resto de las resoluciones o actos del procedimiento deberán notificarse por el medio y en la forma que proceda conforme a lo dispuesto en la Ley 11/2007, de 22 de junio, y en el presente real decreto."

Artículo 37. *Modificación del medio de notificación.*

1. Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la Ley 30/1992, de 26 de noviembre, excepto en los casos en que la notificación por medios electrónicos tenga carácter obligatorio conforme a lo dispuesto en los artículos 27.6 y 28.1 de la Ley 11/2007, de 22 de junio.

2. En la solicitud de modificación del medio de notificación preferente deberá indicarse el medio y lugar para la práctica de las notificaciones posteriores.

3. El cambio de medio a efectos de las notificaciones se hará efectivo para aquellas notificaciones que se emitan desde el día siguiente a la recepción de la solicitud de modificación en el registro del órgano u organismo público actuante.

Artículo 38. *Notificación mediante la puesta a disposición del documento electrónico a través de dirección electrónica habilitada.*

1. Serán válidos los sistemas de notificación electrónica a través de dirección electrónica habilitada siempre que cumplan, al menos, los siguientes requisitos:

a) Acreditar la fecha y hora en que se produce la puesta a disposición del interesado del acto objeto de notificación.

b) Posibilitar el acceso permanente de los interesados a la dirección electrónica correspondiente, a través de una sede electrónica o de cualquier otro modo.

c) Acreditar la fecha y hora de acceso a su contenido.

d) Poseer mecanismos de autenticación para garantizar la exclusividad de su uso y la identidad del usuario.

2. Bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración

General del Estado que no establezcan sistemas de notificación propios. Los ciudadanos podrán solicitar la apertura de esta dirección electrónica, que tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará ésta dirección electrónica, comunicándose así al interesado.

3. Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada a que se refiere el apartado anterior será asignada de oficio y podrá tener vigencia indefinida, conforme al régimen que se establezca por la orden del Ministro de la Presidencia a la que se refiere la disposición final primera. Respecto del resto de direcciones electrónicas habilitadas dicho régimen se establecerá mediante orden del titular del Departamento correspondiente.

Artículo 39. *Notificación mediante recepción en dirección de correo electrónico.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 39. Notificación mediante recepción en dirección de correo electrónico.**
Se podrá acordar la práctica de notificaciones en las direcciones de correo electrónico que los ciudadanos elijan siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación."

Artículo 40. *Notificación por comparecencia electrónica.*

1. La notificación por comparecencia electrónica consiste en el acceso por el interesado, debidamente identificado, al contenido de la actuación administrativa correspondiente a través de la sede electrónica del órgano u organismo público actuante.

2. Para que la comparecencia electrónica produzca los efectos de notificación de acuerdo con el artículo 28.5 de la Ley 11/2007, de 22 de junio, se requerirá que reúna las siguientes condiciones:

a) Con carácter previo al acceso a su contenido, el interesado deberá visualizar un aviso del carácter de notificación de la actuación administrativa que tendrá dicho acceso.

b) El sistema de información correspondiente dejará constancia de dicho acceso con indicación de fecha y hora.

TÍTULO VI

Los documentos electrónicos y sus copias

CAPÍTULO I

Disposiciones comunes sobre los documentos electrónicos

Artículo 41. *Características del documento electrónico.*

1. Los documentos electrónicos deberán cumplir los siguientes requisitos para su validez:

a) Contener información de cualquier naturaleza.

b) Estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

c) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

2. Los documentos administrativos electrónicos deberán, además de cumplir las anteriores condiciones, haber sido expedidos y firmados electrónicamente mediante los sistemas de firma previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y ajustarse a los requisitos de validez previstos en la Ley 30/1992, de 26 de noviembre.

Artículo 42. *Adición de metadatos a los documentos electrónicos.*

1. Se entiende como metadato, a los efectos de este real decreto, cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento.

2. Los documentos electrónicos susceptibles de ser integrados en un expediente electrónico, deberán tener asociados metadatos que permitan su contextualización en el marco del órgano u organismo, la función y el procedimiento administrativo al que corresponde.

Además, se asociará a los documentos electrónicos la información relativa a la firma del documento así como la referencia temporal de los mismos, en la forma regulada en el presente real decreto.

3. La asociación de metadatos a los documentos electrónicos aportados por los ciudadanos o emitidos por la Administración General del Estado o sus organismos públicos será, en todo caso, realizada por el órgano u organismo actuante, en la forma que en cada caso se determine.

4. Los metadatos mínimos obligatorios asociados a los documentos electrónicos, así como la asociación de los datos de firma o de referencia temporal de los mismos, se especificarán en el Esquema Nacional de Interoperabilidad.

5. Una vez asociados los metadatos a un documento electrónico, no podrán ser modificados en ninguna fase posterior del procedimiento administrativo, con las siguientes excepciones:

a) Cuando se observe la existencia de errores u omisiones en los metadatos inicialmente asignados.

b) Cuando se trate de metadatos que requieran actualización, si así lo dispone el Esquema Nacional de Interoperabilidad.

La modificación de los metadatos deberá ser realizada por el órgano competente conforme a la normativa de organización específica, o de forma automatizada conforme a las normas que se establezcan al efecto.

6. Independientemente de los metadatos mínimos obligatorios a que se refiere el apartado 4, los distintos órganos u organismos podrán asociar a los documentos electrónicos metadatos de carácter complementario, para las necesidades de catalogación específicas de su respectivo ámbito de gestión, realizando su inserción de acuerdo con las especificaciones que establezca al respecto el Esquema Nacional de Interoperabilidad. Los metadatos complementarios no estarán sujetos a las prohibiciones de modificación establecidas en el apartado anterior.

Artículo 43. *Copias electrónicas de los documentos electrónicos realizadas por la Administración General del Estado y sus organismos públicos.*

1. Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original.

2. En caso de cambio del formato original, para que una copia electrónica de un documento electrónico tenga la condición de copia auténtica, deberán cumplirse los siguientes requisitos:

a) Que el documento electrónico original, que debe conservarse en todo caso, se encuentre en poder de la Administración.

b) Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

c) Que incluya su carácter de copia entre los metadatos asociados.

d) Que sea autorizada mediante firma electrónica conforme a los sistemas recogidos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

3. Se podrán generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen los requisitos establecidos en los apartados anteriores.

4. Los órganos emisores de los documentos administrativos electrónicos o receptores de los documentos privados electrónicos, o los archivos que reciban los mismos, están obligados a la conservación de los documentos originales, aunque se hubiere procedido a su copiado conforme a lo establecido en el presente artículo, sin perjuicio de lo previsto en el artículo 52.

5. Será considerada copia electrónica auténtica de documentos electrónicos presentados conforme a sistemas normalizados o formularios:

a) La obtenida conforme a lo señalado en los apartados anteriores de este artículo.

b) El documento electrónico, autenticado con la firma electrónica del órgano u organismo destinatario, resultado de integrar el contenido variable firmado y remitido por el ciudadano en el formulario correspondiente empleado en la presentación.

Artículo 44. *Copias electrónicas de documentos en soporte no electrónico.*

1. Las copias electrónicas de los documentos en soporte papel o en otro soporte susceptible de digitalización realizadas por la Administración General del Estado y sus organismos públicos vinculados o dependientes, ya se trate de documentos emitidos por la Administración o documentos privados aportados por los ciudadanos, se realizarán de acuerdo con lo regulado en el presente artículo.

2. A los efectos de lo regulado en este real decreto, se define como «imagen electrónica» el resultado de aplicar un proceso de digitalización a un documento en soporte papel o en otro soporte que permita la obtención fiel de dicha imagen.

Se entiende por «digitalización» el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra, del documento.

3. Cuando sean realizadas por la Administración, las imágenes electrónicas tendrán la naturaleza de copias electrónicas auténticas, con el alcance y efectos previstos en el artículo 46 de la Ley 30/1992, de 26 de noviembre, siempre que se cumplan los siguientes requisitos:

a) Que el documento copiado sea un original o una copia auténtica.

b) Que la copia electrónica sea autorizada mediante firma electrónica utilizando los sistemas recogidos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

c) Que las imágenes electrónicas estén codificadas conforme a alguno de los formatos y con los niveles de calidad y condiciones técnicas especificados en el Esquema Nacional de Interoperabilidad.

d) Que la copia electrónica incluya su carácter de copia entre los metadatos asociados.

e) Que la copia sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

4. No será necesaria la intervención del órgano administrativo depositario del documento administrativo original para la obtención de copias electrónicas auténticas, cuando las imágenes electrónicas sean obtenidas a partir de copias auténticas en papel emitidas cumpliendo los requisitos del artículo 46 de la Ley 30/1992, de 26 de noviembre.

Artículo 45. *Copias en papel de los documentos públicos administrativos electrónicos realizadas por la Administración General del Estado y sus organismos públicos vinculados o dependientes.*

Para que las copias emitidas en papel de los documentos públicos administrativos electrónicos tengan la consideración de copias auténticas deberán cumplirse los siguientes requisitos:

a) Que el documento electrónico copiado sea un documento original o una copia electrónica auténtica del documento electrónico o en soporte papel original, emitidos conforme a lo previsto en el presente real decreto.

b) La impresión en el mismo documento de un código generado electrónicamente u otro sistema de verificación, con indicación de que el mismo permite contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u organismo público emisor.

c) Que la copia sea obtenida conforme a las normas de competencia y procedimiento, que en cada caso se aprueben, incluidas las de obtención automatizada.

Artículo 46. *Destrucción de documentos en soporte no electrónico.*

1. Los documentos originales y las copias auténticas en papel o cualquier otro soporte no electrónico admitido por la ley como prueba, de los que se hayan generado copias electrónicas auténticas, podrán destruirse en los términos y condiciones que se determinen en las correspondientes Resoluciones, si se cumplen los siguientes requisitos:

a) La destrucción requerirá una resolución adoptada por el órgano responsable del procedimiento o, en su caso, por el órgano responsable de la custodia de los documentos, previo el oportuno expediente de eliminación, en el que se determinen la naturaleza específica de los documentos susceptibles de destrucción, los procedimientos administrativos afectados, las condiciones y garantías del proceso de destrucción, y la especificación de las personas u órganos responsables del proceso.

Las resoluciones que aprueben los procesos de destrucción regulados en el artículo 30.4 de la Ley 11/2007, de 22 de junio, requerirán informe previo de la respectiva Comisión Calificadora de Documentos Administrativos y posterior dictamen favorable de la Comisión Superior Calificadora de Documentos Administrativos, sin que, en su conjunto, este trámite de informe pueda ser superior a tres meses. Una vez superado este plazo sin pronunciamiento expreso de ambos órganos, podrá resolverse el expediente de eliminación y procederse a la destrucción.

b) Que no se trate de documentos con valor histórico, artístico o de otro carácter relevante que aconseje su conservación y protección, o en el que figuren firmas u otras expresiones manuscritas o mecánicas que confieran al documento un valor especial.

2. Se deberá incorporar al expediente de eliminación un análisis de los riesgos relativos al supuesto de destrucción de que se trate, con mención explícita de las garantías de conservación de las copias electrónicas y del cumplimiento de las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el Esquema Nacional de Seguridad.

3. La destrucción de cualquier tipo de documento diferente de los previstos en los apartados anteriores, se regirá por lo previsto en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

CAPÍTULO II

Normas específicas relativas a los documentos administrativos electrónicos

Artículo 47. *Referencia temporal de los documentos administrativos electrónicos.*

1. La Administración General del Estado y sus organismos públicos dependientes o vinculados asociarán a los documentos administrativos electrónicos, en los términos del artículo 29.2 de la Ley 11/2007, de 22 de junio, una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) «Marca de tiempo» entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello de tiempo.

b) «Sello de tiempo», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

La información relativa a las marcas y sellos de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad.

2. La relación de prestadores de servicios de certificación electrónica que prestan servicios de sellado de tiempo en la Administración General del Estado, conforme a lo dispuesto en el artículo 29.3 de la Ley 11/2007, de 22 de junio, así como los requisitos que han de cumplirse para dicha admisión, serán regulados mediante el real decreto a que se refiere el artículo 23.3.

CAPÍTULO III

Normas específicas relativas a los documentos electrónicos aportados por los ciudadanos

Artículo 48. *Imágenes electrónicas aportadas por los ciudadanos.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:

"Artículo 48. Imágenes electrónicas aportadas por los ciudadanos.

1. De conformidad con el artículo 35.2 de la Ley 11/2007, de 22 de junio, los interesados podrán aportar al expediente, en cualquier fase del procedimiento, copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada. La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original. La aportación de tales copias implica la autorización a la Administración para que acceda y trate la información personal contenida en tales documentos. Las mencionadas imágenes electrónicas carecerán del carácter de copia auténtica.

2. Las imágenes electrónicas presentadas por los ciudadanos deberán ajustarse a los formatos y estándares aprobados para tales procesos en el Esquema Nacional de Interoperabilidad. En caso de incumplimiento de este requisito, se requerirá al interesado para la subsanación del defecto advertido, en los términos establecidos en el artículo 71 de la Ley 30/1992, de 26 de noviembre.

3. La presentación documental que realicen los interesados en cualquiera de los lugares de presentación establecidos en el artículo 2.1.a), b) y d) del Real Decreto 772/1999, de 7 de mayo, podrá acompañarse de soportes conteniendo documentos electrónicos con los efectos establecidos en el artículo 35.2 de la Ley 11/2007, de 22 de junio.
4. Será de aplicación a las solicitudes de cotejo de las copias aportadas, previstas en el artículo 35.2 de la Ley 11/2007, de 22 de junio, lo establecido en relación con la transmisión de datos en el artículo 2 del presente real decreto."

CAPÍTULO IV

Normas relativas a la obtención de copias electrónicas por los ciudadanos

Artículo 49. *Obtención de copias electrónicas de documentos electrónicos.*

Los ciudadanos podrán ejercer el derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan condición de interesados de acuerdo con lo dispuesto en la normativa reguladora del respectivo procedimiento.

La obtención de la copia podrá realizarse mediante extractos de los documentos o se podrá utilizar otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

Artículo 50. *Obtención de copias electrónicas a efectos de compulsa.*

(Derogado)

Queda derogado este artículo por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicho artículo se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Artículo 50. Obtención de copias electrónicas a efectos de compulsa.**
Cuando los interesados deseen ejercer el derecho regulado en el artículo 8.1 del Real Decreto 772/1999, de 7 de mayo, sobre aportación de copias compulsadas al procedimiento, y siempre que los originales no deban obrar en el procedimiento, la oficina receptora, si cuenta con los medios necesarios, deberá proceder a la obtención de copia electrónica de los documentos a compulsar mediante el procedimiento regulado en el artículo 44 de este real decreto, siempre que se trate de uno de los lugares de presentación mencionados en el artículo 2.1.a), b) y d) del citado real decreto.
Estas copias digitalizadas serán firmadas electrónicamente mediante los procedimientos previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y tendrán el carácter de copia compulsada o cotejada previsto en el artículo 8 del Real Decreto 772/1999, de 7 de mayo, sin que en ningún caso se acredite la autenticidad del documento original, no siéndoles de aplicación el procedimiento de comprobación previsto en el artículo 35.2 de dicha ley."

CAPÍTULO V

Archivo electrónico de documentos

Artículo 51. *Archivo electrónico de documentos.*

1. La Administración General del Estado y sus organismos públicos vinculados o dependientes deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas, que formen parte de un expediente administrativo,

así como aquellos otros que, tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

2. La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria, o mediante la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos así como para la comprobación de la firma electrónica de dichos datos.

Artículo 52. *Conservación de documentos electrónicos.*

1. Los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo de acuerdo con el procedimiento administrativo de que se trate, siendo en todo caso de aplicación, con la excepción regulada de la destrucción de documentos en papel copiados electrónicamente, las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos.

2. Para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados, podrán realizarse operaciones de conversión, de acuerdo con las normas sobre copiado de dichos documentos contenidas en el presente real decreto.

3. Los responsables de los archivos electrónicos promoverán el copiado auténtico con cambio de formato de los documentos y expedientes del archivo tan pronto como el formato de los mismos deje de figurar entre los admitidos en la gestión pública por el Esquema Nacional de Interoperabilidad.

CAPÍTULO VI

Expediente electrónico

Artículo 53. *Formación del expediente electrónico.*

1. La formación de los expedientes electrónicos es responsabilidad del órgano que disponga la normativa de organización específica y, de no existir previsión normativa, del encargado de su tramitación.

2. Los expedientes electrónicos que deban ser objeto de remisión o puesta a disposición se formarán ajustándose a las siguientes reglas:

a) Los expedientes electrónicos dispondrán de un código que permita su identificación unívoca por cualquier órgano de la Administración en un entorno de intercambio interadministrativo.

b) El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado electrónicamente mediante los sistemas previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y en los términos del artículo 32.2 de la citada ley.

c) Con el fin de garantizar la interoperabilidad de los expedientes, tanto su estructura y formato como las especificaciones de los servicios de remisión y puesta a disposición se sujetarán a lo que se establezca al respecto por el Esquema Nacional de Interoperabilidad.

d) Los expedientes electrónicos estarán integrados por documentos electrónicos, que podrán formar parte de distintos expedientes, pudiendo incluir asimismo otros expedientes electrónicos si así lo requiere el procedimiento. Excepcionalmente, cuando la naturaleza o la extensión de determinados documentos a incorporar al expediente no permitan o dificulten notablemente su inclusión en el mismo conforme a los estándares y procedimientos establecidos, deberán incorporarse al índice del expediente sin perjuicio de su aportación separada.

e) Los documentos que se integran en el expediente electrónico se ajustarán al formato o formatos de larga duración, accesibles en los términos que determine el Esquema Nacional de Interoperabilidad.

Disposición adicional primera. *Procedimientos especiales.*

1. **(Derogado)**

2. **(Derogado)**

3. Lo dispuesto en el presente real decreto se aplicará supletoriamente al régimen especial previsto en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido y en la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas contenidas en el citado real decreto. Este régimen jurídico especial será aplicable a cualesquiera copias electrónicas de facturas que deban remitirse a los órganos y organismos de la Administración General del Estado.

4. **(Derogado)**

Quedan derogados los apartados 1, 2 y 4 por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dichos apartados 1, 2 y 4 se mantendrán en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:

"1. Lo dispuesto en este real decreto se entiende sin perjuicio de la regulación especial contenida en la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público y sus normas de desarrollo en relación con el perfil del contratante, Plataforma de Contratación del Estado y uso de medios electrónicos en los procedimientos relacionados con la contratación pública.

2. La aplicación de las disposiciones de este real decreto sobre gestión electrónica de procedimientos en materia tributaria, de seguridad social y desempleo y de régimen jurídico de los extranjeros en España, se efectuará de conformidad con lo establecido en las disposiciones adicionales quinta, sexta, séptima y decimonovena de la Ley 30/1992, de 26 de noviembre.

3. Lo dispuesto en el presente real decreto se aplicará supletoriamente al régimen especial previsto en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido y en la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas contenidas en el citado real decreto. Este régimen jurídico especial será aplicable a cualesquiera copias electrónicas de facturas que deban remitirse a los órganos y organismos de la Administración General del Estado.

4. Lo dispuesto en este real decreto se entiende sin perjuicio de la regulación contenida en los reales decretos 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado» y 1979/2008, de 28 de noviembre, por el que se regula la edición electrónica del «Boletín Oficial del Registro Mercantil»."

Disposición adicional segunda. *Función estadística.*

Lo dispuesto en el artículo 2 no se aplicará a la recogida de datos prevista en el Capítulo II de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

Disposición adicional tercera. *Directorio de sedes electrónicas.*

(Derogada)

Queda derogada por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. y por la disposición derogatoria única.g) de la Ley 40/2015, de 1 de octubre. Ref. BOE-A-2015-10566. a partir del 2 de octubre de 2016. No obstante, esta disposición se mantendrá en vigor hasta que produzcan efectos las previsiones de la Ley 39/2015, relativas a la materia que se deroga, según establece su disposición final 7.

Redacción anterior:

"**Disposición adicional tercera. Directorio de sedes electrónicas.**
En el plazo de 6 meses, contados a partir de la entrada en vigor de este real decreto, el Ministerio de la Presidencia publicará en su sede electrónica el Directorio de sedes electrónicas a que se refiere el artículo 8."

Disposición adicional cuarta. *Conservación de la identificación de direcciones electrónicas.*

Sin perjuicio de lo establecido, con carácter general, en el artículo 17.2, las direcciones electrónicas actualmente existentes de los organismos públicos que gocen de un alto nivel de conocimiento público, podrán ser mantenidas con la misma identificación electrónica.

Disposición adicional quinta. *Plataforma de verificación de certificados de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

De conformidad con las facultades que otorga a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social en relación con la disposición adicional cuarta de la Ley 59/2003, de 19 de diciembre, de firma electrónica, la plataforma de verificación de certificados desarrollada por esta entidad se integrará en el sistema nacional de verificación de certificados regulado en el artículo 25.3 del presente real decreto, cumpliendo con lo especificado en el artículo 25.4.

El Ministerio de la Presidencia y la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda adoptarán las medidas para conseguir la permanente y perfecta coordinación operativa y la coherencia técnica de ambas plataformas de verificación, con la finalidad de asegurar su interoperabilidad y garantizar el mejor servicio a las Administraciones y los ciudadanos.

Disposición adicional sexta. *Ausencia de impacto presupuestario.*

La aplicación de las previsiones contenidas en este real decreto no deberá ocasionar incremento del gasto público ni disminución de los ingresos públicos. Por tanto, los departamentos ministeriales afectados deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

Disposición transitoria primera. *Sistemas de firma electrónica.*

(Derogada)

Queda derogada esta disposición por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicha disposición se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Disposición transitoria primera. Sistemas de firma electrónica.**
1. En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad podrán seguir utilizándose los medios actualmente admitidos de identificación y autenticación. Dichos esquemas establecerán los plazos de aprobación de las relaciones de medios admitidos así como los plazos máximos de utilización de los medios que habiendo sido utilizados no se adecúen a las prescripciones de los mismos.
2. En particular, podrá seguir utilizándose para los usos previstos en este real decreto y con los mismos efectos jurídicos que el sello electrónico, la firma electrónica de persona jurídica o del

titular del órgano administrativo con observancia de lo dispuesto en la normativa correspondiente."

Disposición transitoria segunda. *Condiciones de seguridad de las plataformas de verificación.*

(Derogada)

Queda derogada por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. y por la disposición derogatoria única.g) de la Ley 40/2015, de 1 de octubre. Ref. BOE-A-2015-10566. a partir del 2 de octubre de 2016. No obstante, esta disposición se mantendrá en vigor hasta que produzcan efectos las previsiones de la Ley 39/2015, relativas a la materia que se deroga, según establece su disposición final 7.

Redacción anterior:
"**Disposición transitoria segunda. Condiciones de seguridad de las plataformas de verificación.**
En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad, seguirán teniendo validez los sistemas y servicios de verificación existentes y operativos a la entrada en vigor de este real decreto. Los certificados vinculados a dichos sistemas o servicios podrán utilizarse en los procedimientos que expresamente los prevean."

Disposición transitoria tercera. *Sistema de notificación electrónica regulado en el artículo 38.2.*

(Derogada)

Queda derogada esta disposición por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. a partir del 2 de octubre de 2016, según establece su disposición final 7. No obstante, dicha disposición se mantendrá en vigor hasta que produzcan efectos las previsiones de la citada ley relativas a la materia que se deroga.

Redacción anterior:
"**Disposición transitoria tercera. Sistema de notificación electrónica regulado en el artículo 38.2.**
Mientras no se proceda a dictar la regulación del Sistema de notificación electrónica regulado en el artículo 38.2, de acuerdo con la disposición final primera, la función prevista en el sistema de notificación se realizará a través de los servicios autorizados, de conformidad con la Orden PRE 1551/2003, de 10 junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por la que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos."

Disposición transitoria cuarta. *Adaptación de sedes electrónicas.*

(Derogada)

Queda derogada por la disposición derogatoria única.2.g) de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. y por la disposición derogatoria única.g) de la Ley 40/2015, de 1 de octubre. Ref. BOE-A-2015-10566. No obstante, esta disposición se mantendrá en vigor hasta

que produzcan efectos las previsiones de la Ley 39/2015, relativas a la materia que se deroga, según establece su disposición final 7.

Redacción anterior:
"**Disposición transitoria cuarta. Adaptación de sedes electrónicas.**
En tanto no se aprueben los Esquemas Nacionales de Interoperabilidad y de Seguridad, la creación de sedes deberá ir acompañada de un informe en el que se acredite el cumplimiento de las condiciones de confidencialidad, disponibilidad e integridad de las informaciones y comunicaciones que se realicen a través de las mismas."

Disposición transitoria quinta. *Adaptación en la Administración General del Estado en el Exterior.*

La aplicación de lo dispuesto en este real decreto a la Administración General del Estado en el Exterior se efectuará según los medios de identificación y autenticación de los ciudadanos, los canales electrónicos y condiciones de funcionamiento que en cada momento se encuentren disponibles.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto, y especialmente:

a) El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

b) Los artículos 14 a 18 del Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

Disposición final primera. *Sistema de notificación electrónica regulado en el artículo 38.2.*

Por orden del Ministro de la Presidencia se establecerá el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2, que deberá ajustarse a las previsiones del mismo.

Disposición final segunda. *Punto de acceso general.*

En el plazo de 3 meses desde la entrada en vigor de este real decreto, el Ministro de la Presidencia dictará las disposiciones necesarias para la constitución del punto de acceso general de la Administración General del Estado regulado en el artículo 9.

Disposición final tercera. *Registros electrónicos.*

Los registros telemáticos existentes a la entrada en vigor de la Ley 11/2007, de 22 de junio, afectados por el apartado 2 de la disposición transitoria única de la citada ley, ajustarán su funcionamiento a lo establecido en este real decreto dentro de los seis meses siguientes a su entrada en vigor.

La adaptación a lo dispuesto en el presente real decreto se realizará mediante orden ministerial o, en su caso, resolución del titular del correspondiente organismo público, por la que se explicite el cumplimiento de lo dispuesto en el artículo 27.

Disposición final cuarta. *Sedes electrónicas.*

Los puntos de acceso electrónico pertenecientes a la Administración General del Estado o sus organismos públicos dependientes o vinculados en los que se desarrollan actualmente comunicaciones con terceros, propias de sede electrónica, deberán adaptarse, en el plazo de cuatro meses, contados a partir de la entrada en vigor de este real decreto, a lo dispuesto

en el mismo para las sedes o, en su caso, subsedes, electrónicas, sin perjuicio de lo previsto en las disposiciones transitorias primera y segunda de este real decreto y en la disposición final tercera.2 de la Ley 11/2007, de 22 de junio.

Disposición final quinta. *Habilitación para el desarrollo normativo.*

Se habilita a los Ministros de la Presidencia, Economía y Hacienda e Industria, Turismo y Comercio para dictar las disposiciones que sean necesarias para el desarrollo de este real decreto, en el ámbito de sus respectivas competencias.

Disposición final sexta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 31

Ley 59/2003, de 19 de diciembre, de firma electrónica

Jefatura del Estado
«BOE» núm. 304, de 20 de diciembre de 2003
Última modificación: 2 de octubre de 2015
Referencia: BOE-A-2003-23399

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

EXPOSICIÓN DE MOTIVOS

I

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado real decreto ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el Diario Oficial de las Comunidades Europeas.

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto Ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto Ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Asimismo, debe destacarse que la ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el "Diario Oficial de las Comunidades Europeas" o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.

Adicionalmente, la ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

III

Esta ley se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto Ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

Una de las novedades que la ley ofrece respecto del Real Decreto Ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se trata simplemente de la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación.

Asimismo, es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.

El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Si bien se recogen fielmente en la ley los conceptos de "acreditación" de prestadores de servicios de certificación y de "conformidad" de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características - acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

Asimismo, otra novedad es el establecimiento en la ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos.

Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados ; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Con la expresión "giro o tráfico ordinario" de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. Por último, debe recalcarse que, aunque el "giro o tráfico ordinario" sea un término acuñado por el derecho mercantil, la regulación sobre los certificados de personas jurídicas no sólo se aplica a las sociedades mercantiles, sino a cualquier tipo de persona jurídica que quiera hacer uso de la firma electrónica en su actividad.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la ley es el acogimiento explícito que se efectúa de las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica.

Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los

Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos.

Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

IV

La ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

2. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

Artículo 2. *Prestadores de servicios de certificación sujetos a la ley.*

1. Esta ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

2. Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

3. Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

4. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

5. Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Artículo 3. *Firma electrónica, y documentos firmados electrónicamente.*

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas

comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos.

Téngase en cuenta que el apartado 11 añadido por la disposición final 2 de la Ley 39/2015, de 1 de octubre. Ref. BOE-A-2015-10565. entra en vigor el 2 de octubre de 2016, según establece su disposición final 7.

Artículo 4. *Empleo de la firma electrónica en el ámbito de las Administraciones públicas.*

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Artículo 5. *Régimen de prestación de los servicios de certificación.*

1. La prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los

servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

TÍTULO II

Certificados electrónicos

CAPÍTULO I

Disposiciones generales

Artículo 6. *Concepto de certificado electrónico y de firmante.*

1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

2. El firmante es la persona que utiliza un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Artículo 7. *Certificados electrónicos de personas jurídicas.*

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica o, en su caso, de los medios de acceso a ellos será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

5. Lo dispuesto en este artículo no será de aplicación a los certificados que sirvan para verificar la firma electrónica del prestador de servicios de certificación con la que firme los certificados electrónicos que expida.

6. Lo dispuesto en este artículo no será de aplicación a los certificados que se expidan a favor de las Administraciones públicas, que estarán sujetos a su normativa específica.

Artículo 8. *Extinción de la vigencia de los certificados electrónicos.*

1. Son causas de extinción de la vigencia de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.

b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante ; fallecimiento, o extinción de la personalidad jurídica del representado ; incapacidad sobrevenida, total o parcial, del firmante o de su representado ; terminación de la representación ; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cinco años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 9. *Suspensión de la vigencia de los certificados electrónicos.*

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b) Resolución judicial o administrativa que lo ordene.

c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.

d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 10. *Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.*

1. El prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

2. El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima,

extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

CAPÍTULO II

Certificados reconocidos

Artículo 11. *Concepto y contenido de los certificados reconocidos.*

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Artículo 12. *Obligaciones previas a la expedición de certificados reconocidos.*

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.

c) Asegurarse de que el firmante tiene el control exclusivo sobre el uso de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Artículo 13. *Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.*

1. La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

4. Lo dispuesto en los apartados anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

5. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Artículo 14. *Equivalencia internacional de certificados reconocidos.*

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III

El documento nacional de identidad electrónico

Artículo 15. *Documento nacional de identidad electrónico.*

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. *Requisitos y características del documento nacional de identidad electrónico.*

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

TÍTULO III

Prestación de servicios de certificación

CAPÍTULO I

Obligaciones

Artículo 17. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la

firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 18. *Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.*

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el firmante controle de modo exclusivo el uso de sus datos de creación de firma.

Solo los prestadores de servicios de certificación que expidan certificados reconocidos podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No podrán duplicar los datos de creación de firma para ninguna otra finalidad.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos, o, en su caso, de los medios que los protegen, así como información sobre los dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6.º Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

Artículo 19. *Declaración de prácticas de certificación.*

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

Artículo 20. *Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.*

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante. Si el prestador de servicios gestiona los datos de creación de firma en nombre del firmante, deberá custodiarlos y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante.

f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

2. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

Artículo 21. *Cese de la actividad de un prestador de servicios de certificación.*

1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas ; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia.

La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

2. El prestador de servicios de certificación que expida certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

3. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f). Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.

CAPÍTULO II

Responsabilidad

Artículo 22. *Responsabilidad de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta ley.

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b) al d) del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

5. La regulación contenida en esta ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores.

Artículo 23. *Limitaciones de responsabilidad de los prestadores de servicios de certificación.*

1. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a) No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

2. En el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta ley.

3. Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1.

4. El prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

6. La exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia.

TÍTULO IV

Dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica

CAPÍTULO I

Dispositivos de firma electrónica

Artículo 24. *Dispositivos de creación de firma electrónica.*

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Artículo 25. *Dispositivos de verificación de firma electrónica.*

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

CAPÍTULO II

Certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica

Artículo 26. *Certificación de prestadores de servicios de certificación.*

1. La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

2. La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

4. La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica.

Artículo 27. *Certificación de dispositivos seguros de creación de firma electrónica.*

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea" y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

Artículo 28. *Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.*

1. Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea".

2. Se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo.

TÍTULO V

Supervisión y control

Artículo 29. *Supervisión y control.*

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

2. El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. El Ministerio de Ciencia y Tecnología podrá acordar las medidas apropiadas para el cumplimiento de esta ley y sus disposiciones de desarrollo.

4. El Ministerio de Ciencia y Tecnología podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de certificación que le asigna esta ley.

5. Podrá requerirse la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos. En este caso, los prestadores de servicios correrán con los gastos que ocasione esta evaluación.

Artículo 30. *Deber de información y colaboración.*

1. Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

En particular, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas.

2. Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VI

Infracciones y sanciones

Artículo 31. *Infracciones.*

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e) El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.

4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

Artículo 32. *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.

La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito.

Artículo 33. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

a) La existencia de intencionalidad o reiteración.

b) La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.

c) La naturaleza y cuantía de los perjuicios causados.

d) Plazo de tiempo durante el que se haya venido cometiendo la infracción e) El beneficio que haya reportado al infractor la comisión de la infracción.

f) Volumen de la facturación a que afecte la infracción cometida.

Artículo 34. *Medidas provisionales.*

1. En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios de certificación y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertencia al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en este artículo podrán ser acordadas antes de la iniciación del expediente sancionador.

Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los 15 días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 35. *Multa coercitiva.*

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 36. *Competencia y procedimiento sancionador.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

Disposición adicional primera. *Fe pública y uso de firma electrónica.*

1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

Disposición adicional segunda. *Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.*

1. En el ámbito de la certificación de dispositivos de creación de firma, corresponderá al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología la imposición de sanciones por la comisión, por los organismos de certificación de dispositivos seguros de creación de firma electrónica o por la entidad que los acredite, de las infracciones graves previstas en los párrafos e), f) y g) del apartado segundo del artículo 31 de la Ley 21/1992, de 16 de julio, de Industria, y de las infracciones leves indicadas en el párrafo a) del apartado 3 del artículo 31 de la citada ley que cometan en el ejercicio de actividades relacionadas con la certificación de firma electrónica.

2. Cuando dichas infracciones merezcan la calificación de infracciones muy graves, serán sancionadas por el Ministro de Ciencia y Tecnología.

Disposición adicional tercera. *Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.*

Podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda.

Disposición adicional cuarta. *Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.*

Lo dispuesto en esta ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Disposición adicional quinta. *Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.*

Se añaden apartado doce al artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, con la siguiente redacción.

> "Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica."

Disposición adicional sexta. *Régimen jurídico del documento nacional de identidad electrónico.*

1. Sin perjuicio de la aplicación de la normativa vigente en materia del documento nacional de identidad en todo aquello que se adecue a sus características particulares, el documento nacional de identidad electrónico se regirá por su normativa específica.
2. El Ministerio de Ciencia y Tecnología podrá dirigirse al Ministerio del Interior para que por parte de éste se adopten las medidas necesarias para asegurar el cumplimiento de las obligaciones que le incumban como prestador de servicios de certificación en relación con el documento nacional de identidad electrónico.

Disposición adicional séptima. *Emisión de facturas por vía electrónica.*

Lo dispuesto en esta ley se entiende sin perjuicio de las exigencias derivadas de las normas tributarias en materia de emisión de facturas por vía electrónica.

Disposición adicional octava. *Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

Uno. Adición de un nuevo apartado 3 al artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Se añade un apartado 3 con el siguiente texto:

> "3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.
>
> A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:
>
> a) Las características del servicio que se va a proporcionar.
>
> b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.
>
> c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y d) El

procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional."

Dos. Los apartados 2, 3 y 4 del artículo 38 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se redactan en los siguientes términos:

"2. Son infracciones muy graves:

a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.

c) El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

a) El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.

b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.

c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.

f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

g) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley.

h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.

i) El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

a) La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones

de Internet que empleen para la prestación de servicios de la sociedad de la información.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g) El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave."

Tres. Modificación del artículo 43, apartado 1, segundo párrafo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El segundo párrafo del apartado 1 del artículo 43 queda redactado como sigue:

"No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta ley."

Cuatro. Modificación del artículo 43, apartado 2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El apartado 2 del artículo 43 queda redactado como sigue:

"2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses."

Disposición adicional novena. *Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.*

Los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas con discapacidad y de la tercera edad, las cuales no podrán ser en ningún caso discriminadas en el ejercicio de los derechos y facultades reconocidos en esta ley por causas basadas en razones de discapacidad o edad avanzada.

Disposición adicional décima. *Modificación de la Ley de Enjuiciamiento Civil.*

Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:

"Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica."

Disposición adicional undécima. *Resolución de conflictos.*

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.

Disposición transitoria primera. *Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta ley.*

Los certificados electrónicos que hayan sido expedidos por prestadores de servicios de certificación en el marco del Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez.

Disposición transitoria segunda. *Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley.*

Los prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley deberán comunicar al Ministerio de Ciencia y Tecnología su actividad y las características de los servicios que presten en el plazo de un mes desde la referida entrada en vigor. Esta información será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

Disposición final primera. *Fundamento constitucional.*

Esta ley se dicta al amparo del artículo 149.1.8.ª, 18.ª, 21.ª y 29.ª de la Constitución.

Disposición final segunda. *Desarrollo reglamentario.*

1. El Gobierno adaptará la regulación reglamentaria del documento nacional de identidad a las previsiones de esta ley.

2. Así mismo, se habilita al Gobierno para dictar las demás disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta ley.

Disposición final tercera. *Entrada en vigor.*

La presente ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

§ 32

Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

Ministerio del Interior
«BOE» núm. 307, de 24 de diciembre de 2005
Última modificación: 30 de mayo de 2015
Referencia: BOE-A-2005-21163

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en su artículo 9, reconoce el derecho de todos los españoles a que se les expida el Documento Nacional de Identidad, al que se atribuye el valor suficiente para acreditar, por sí solo, la identidad de las personas y le otorga la protección que a los documentos públicos y oficiales es reconocida por el ordenamiento jurídico.

La misma norma dispone la obligatoriedad del Documento Nacional de Identidad para los mayores de catorce años, salvo en los supuestos en que, conforme a lo previsto en la Ley, haya de ser sustituido por otro documento, y establece también que en el mismo figurarán la fotografía y la firma del titular, así como los datos personales que se determinen reglamentariamente.

En cuanto a la competencia para su expedición y gestión, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, atribuye al Cuerpo Nacional de Policía, la de la expedición del Documento Nacional de Identidad, al recogerla expresamente entre las funciones que encomienda a este Instituto Policial, el cual la misma Ley dispone que dependerá del Ministerio del Interior.

Por otra parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.

La misma Ley, en el apartado primero de la disposición final segunda dispone que el Gobierno adaptará la regulación reglamentaría del Documento Nacional de Identidad a las previsiones de la referida Ley.

Asimismo, ha de señalarse que la normativa reglamentaria que regula los distintos aspectos del Documento Nacional de Identidad se encuentra dispersa en distintas disposiciones y data, en parte, de fechas anteriores a la vigencia de la Constitución, lo que genera disfunciones a la hora de su aplicación, derivadas tanto de la propia antigüedad de las normas, como de la dispersión de estas.

En este contexto, y a la vista del mandato legal contenido en la Ley 59/2003, antes citada, resulta imprescindible acometer la adecuación y ordenación de la normativa que regula el referido Documento, abordando aquellos aspectos derivados de las nuevas utilidades que se le atribuyen.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros, en su reunión del día 23 de diciembre de 2005,

D I S P O N G O :

Artículo 1. *Naturaleza y funciones.*

1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.

2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.

3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento.

Artículo 2. *Derecho y obligación de obtenerlo.*

1. Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo cuando fueren requeridas para ello por la Autoridad o sus Agentes.

Artículo 3. *Órgano competente para la expedición y gestión.*

1. Será competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

2. El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, de 13 de septiembre, de Protección de Datos de Carácter Personal.

Artículo 4. *Procedimiento de expedición.*

1. El Documento Nacional de Identidad se expedirá a solicitud del interesado en la forma y lugares que al efecto se determinen, para lo cual deberá aportar los documentos que se establecen en el artículo 5.1 de este Real Decreto.

2. En orden a facilitar a los ciudadanos la obtención del Documento Nacional de Identidad, el Ministerio del Interior en colaboración con el Ministerio de Administraciones Públicas adoptará las medidas oportunas para el fomento de la cooperación de los distintos órganos de las Administraciones Públicas con la Dirección General de la Policía.

Artículo 5. *Requisitos para la expedición.*

1. Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

a) Certificación literal de nacimiento expedida por el Registro Civil correspondiente. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de seis meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme blanco y liso, tomada de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.

c) Certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del documento nacional de identidad.

d) Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

2. Excepcionalmente, en los supuestos en que, por circunstancias ajenas al solicitante, no pudiera ser presentado alguno de los documentos a que se refiere el apartado primero de este artículo, y siempre que se acrediten por otros medios, suficientes a juicio del responsable del órgano encargado de la expedición, los datos que consten en tales documentos, se le podrá expedir un Documento Nacional de Identidad con la validez que se indica en el artículo siguiente.

3. En el momento de la solicitud, al interesado se le recogerán las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos.

Artículo 6. *Validez.*

1. Con carácter general el documento nacional de identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

a) Dos años cuando el solicitante no haya cumplido los cinco años de edad.

b) Cinco años, cuando el titular haya cumplido los cinco años de edad y no haya alcanzado los treinta al momento de la expedición o renovación.

c) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.

d) Permanente cuando el titular haya cumplido los setenta años.

2. De forma excepcional se podrá otorgar validez distinta al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

a) Permanente, a personas mayores de treinta años que acrediten la condición de gran inválido.

b) Por un año en los supuestos del apartado segundo del artículo 5 y del mismo apartado del artículo 7 siempre que, en éste último caso, no se puedan aportar los documentos justificativos que acrediten la variación de los datos.

3. No obstante lo dispuesto en este artículo, en cuanto a la validez de la utilidad informática prevista en el artículo 1.4 se estará a lo que específicamente se establece al respecto en el artículo 12 de este Real Decreto.

Artículo 7. *Renovación.*

1. Transcurrido el período de validez que para cada supuesto se contempla en el artículo anterior, el Documento Nacional de Identidad se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la renovación del mismo.

Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar una fotografía con las características señaladas en el artículo 5.1.b). También se le recogerán las impresiones dactilares que se refieren en el apartado tercero del mismo artículo.

2. Independientemente de los supuestos del apartado anterior se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además de lo establecido en el apartado anterior, los documentos justificativos que acrediten dicha variación.

Artículo 8. *Expedición de duplicados.*

1. El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el apartado primero del artículo anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

2. Los documentos sustituidos perderán el carácter de Documento Nacional de Identidad, así como los efectos que el ordenamiento jurídico atribuye a éste con respecto a su titular.

Artículo 9. *Entrega del Documento Nacional de Identidad.*

1. La entrega del documento nacional de identidad deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas. En el momento de la entrega del documento nacional de identidad se proporcionará la información a que se refiere el artículo 18.b) de la Ley 59/2003, de 19 de diciembre.

2. La activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema.

3. Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

Artículo 10. *Características de la tarjeta soporte.*

1. El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por el Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos conducentes a la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación. Llevará incorporado un chip electrónico al objeto de posibilitar la utilidad informática a que se refiere el artículo 1.4 de este Real Decreto.

2. La tarjeta soporte llevará estampados en el anverso, de forma destacada y preeminente los literales «Documento Nacional de Identidad», «España» y «Ministerio del Interior».

Artículo 11. *Contenido.*

1. El Documento Nacional de Identidad recogerá gráficamente los siguientes datos de su titular:

En el anverso:

Apellidos y nombre.
Fecha de nacimiento.
Sexo.
Nacionalidad.
Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal.
Fotografía.
Firma.

En el reverso:

Lugar de nacimiento.
Provincia-Nación.
Nombre de los padres.
Domicilio.
Lugar de domicilio.
Provincia.
Nación.
Caracteres OCR-B de lectura mecánica.

Los datos de filiación se reflejarán en los mismos términos en que consten en la certificación a la que se alude en el artículo 5.1.a) de este Real Decreto, excepto en el campo de caracteres OCR-B de lectura mecánica, en que por aplicación de acuerdos o convenios internacionales la transcripción literal de aquellos datos impida o dificulte la lectura mecánica y finalidad de aquellos caracteres.

2. Igualmente constarán los siguientes datos referentes al propio Documento y a la tarjeta soporte:

Fecha de caducidad
Número de soporte.

3. Los textos fijos se expresarán en castellano y los expedidos en territorio de aquellas Comunidades Autónomas que tengan otra lengua oficial, serán también expresados en esta.

4. El chip incorporado a la tarjeta soporte contendrá:

Datos de filiación del titular.
Imagen digitalizada de la fotografía.
Imagen digitalizada de la firma manuscrita.
Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este Real Decreto.
Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

Artículo 12. *Validez de los certificados electrónicos.*

1. Con independencia de lo que establece el artículo 6.1 sobre la validez del documento nacional de identidad, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a cinco años.

A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. Para la solicitud de un nuevo certificado deberá mediar la presencia física del titular en la forma y con los requisitos que se

determinen por el Ministerio del Interior, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre.

2. El cumplimiento del período establecido en el apartado anterior implicará la inclusión de los certificados en la lista de certificados revocados que será mantenida por la Dirección General de la Policía, bien directamente o a través de las entidades a las que encomiende su gestión.

3. La pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

4. También serán causas de extinción de la vigencia del certificado reconocido las establecidas en la Ley 59/2003, de 19 de diciembre, que resulten de aplicación, y, entre otras, el fallecimiento del titular del Documento Nacional de Identidad electrónico.

5. En los supuestos previstos en el artículo 8.1 de este Real Decreto, el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios que al efecto habilite la misma, al objeto de su revocación.

Artículo 13. *Declaración de Prácticas y Políticas de Certificación.*

De acuerdo y en cumplimiento del artículo 19 de la Ley 59/2003, de 19 de diciembre, el Ministerio del Interior formulará una Declaración de Prácticas y Políticas de Certificación. Dicha Declaración de Prácticas y Políticas de Certificación estará disponible al público de manera permanente y fácilmente accesible en la página de Internet del Ministerio del Interior.

Disposición adicional primera. *Documento de sustitución del Documento Nacional de Identidad en supuestos de retirada de éste.*

En los supuestos en que, de acuerdo con las previsiones establecidas en las Leyes, sea acordada por la Autoridad competente la retirada temporal de Documento Nacional de Identidad por los órganos encargados de la expedición de éste, se procederá a dotar al interesado de un documento identificador que tendrá las características y funcionalidades que determine el Ministerio del Interior, atendiendo a las causas de su retirada.

Disposición adicional segunda. *Documento Nacional de Identidad de los menores de edad.*

La posesión del Documento Nacional de Identidad por los menores de edad no supone, por sí sola, autorización para desplazarse fuera del territorio nacional, debiendo ser suplida, a estos efectos, con la correspondiente autorización de quien ejerza la patria potestad o tutela.

Disposición adicional tercera. *Imposibilidad de expedición o renovación del Documento Nacional de Identidad.*

Cuando exista imposibilidad manifiesta para la expedición del Documento Nacional de Identidad, y sin perjuicio de que por las Autoridades y Órganos correspondientes se compruebe la personalidad del interesado por cualesquiera otros medios, excepcionalmente podrá sustituirse aquél por certificaciones anuales en las que consten los motivos de tal imposibilidad, que en los supuestos de renovación tendrán únicamente el fin de prorrogar la validez del Documento caducado.

Disposición adicional cuarta. *Remisión de información por vía telemática.*

1. La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.

2. En estos casos, por Orden del Ministro del Interior se establecerá el régimen de aportación de dichos documentos.

Disposición transitoria única. *Validez de los Documentos Nacionales de Identidad expedidos o renovados de conformidad con la normativa anterior a este Real Decreto y proceso de sustitución.*

1. Los Documentos Nacionales de Identidad ya emitidos o los que se continúen expidiendo por el sistema anterior conforme a la normativa existente a la entrada en vigor de este Real Decreto seguirán siendo válidos y eficaces de conformidad con dicha normativa en tanto no se proceda a su sustitución por el Documento Nacional de Identidad de acuerdo con lo que se establece en el apartado siguiente de esta disposición.

2. La Dirección General de la Policía programará y organizará, temporal y territorialmente el proceso de sustitución de las tarjetas soporte del Documento Nacional de Identidad emitidas con anterioridad a la entrada en vigor de este Real Decreto por el nuevo Documento Nacional de Identidad, pudiendo establecerse por razones de interés público programaciones especiales para determinados colectivos.

3. Sólo se podrá solicitar la expedición del nuevo Documento Nacional de Identidad en el marco de la programación a que se hace referencia en el apartado anterior.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas las siguientes disposiciones: Decreto 196/1976, de 6 de febrero, por el que se regula el Documento Nacional de Identidad, y las modificaciones llevadas a cabo en el mismo a través de los Reales Decretos 1189/1978, de 2 de junio; 2002/1979, de 20 de julio; 2091/1982, de 12 de agosto; y 1245/1985, de 17 de julio.

2. Asimismo, quedan derogadas todas aquellas normas de igual o inferior rango que se opongan a lo preceptuado en este Real Decreto.

Disposición final primera. *Título competencial.*

Este Real Decreto se dicta al amparo de las competencias atribuidas al Estado por el artículo 149.1.8.ª,18.ª, 21.ª y 29.ª de la Constitución.

Disposición final segunda. *Desarrollo.*

1. El Ministerio del Interior adoptará las disposiciones necesarias para dar cumplimiento a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, en materia de creación y modificación de ficheros de titularidad pública.

2. Se habilita a los Ministros del Interior, de Justicia, de Economía y Hacienda, de Industria, Turismo y Comercio y de Administraciones Públicas para que dicten, en el ámbito de sus respectivas competencias, cuantas disposiciones sean necesarias para el desarrollo y aplicación de este Real Decreto.

Disposición final tercera. *Tasas.*

El Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad.

Disposición final cuarta. *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», excepto lo relativo al artículo 1.4 que entrará en vigor cuando lo haga el nuevo formato y diseño del Documento Nacional de Identidad.

§ 33

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones

Jefatura del Estado
«BOE» núm. 114, de 10 de mayo de 2014
Última modificación: 7 de marzo de 2016
Referencia: BOE-A-2014-4950

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, transpuso al ordenamiento jurídico español el marco regulador de las comunicaciones electrónicas aprobado por la Unión Europea en el año 2002, profundizando en los principios de libre competencia y mínima intervención administrativa consagrados en la normativa anterior.

Desde su aprobación, la Ley 32/2003, de 3 de noviembre, ha sido objeto de diversas modificaciones tendentes a garantizar la aparición y viabilidad de nuevos operadores, la protección de los derechos de los usuarios y la supervisión administrativa de aquellos aspectos relacionados con el servicio público, el dominio público y la defensa de la competencia.

La última de estas modificaciones, efectuada a través del real decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista, ha incorporado al ordenamiento jurídico español el nuevo marco regulador europeo en materia de comunicaciones electrónicas del año 2009.

Este nuevo marco europeo está compuesto por la Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Derechos de los Usuarios), y la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Mejor Regulación), y a partir del mismo se introducen en la Ley medidas destinadas a crear un marco adecuado para la realización de inversiones en el despliegue de redes de nueva generación, de modo que se permita a los operadores ofrecer servicios innovadores y tecnológicamente más adecuados a las necesidades de los ciudadanos.

II

Las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir al crecimiento, la productividad, el empleo, y por tanto, al desarrollo económico y al bienestar social, afectando directamente al círculo de protección de los intereses generales.

Actualmente, la evolución tecnológica nos sitúa en una nueva etapa –la de extensión de las redes de nueva generación–, que obliga a los poderes públicos a reflexionar sobre la importancia de la función regulatoria.

La situación económica y financiera que afecta a una gran parte de los países desarrollados, la necesidad actual de fomentar la inversión e impulsar la competencia, son elementos esenciales a considerar en la revisión del marco regulador.

El sector de las telecomunicaciones, sujeto a un proceso de permanente innovación tecnológica, necesita de constantes e ingentes inversiones, lo que requiere acometer proyectos de gran envergadura que pueden verse afectados si se exigieran en condiciones distintas de despliegue de redes y de comercialización de servicios en los diferentes ámbitos territoriales.

La Agenda Digital para Europa, principal instrumento para el cumplimiento de los objetivos de la Estrategia Europa 2020, persigue que para 2020 todos los europeos tengan la posibilidad de acceder a conexiones de banda ancha a una velocidad como mínimo de 30 Mbps, y que, al menos, un 50 % de los hogares europeos estén abonados a conexiones de banda ancha superiores a 100 Mbps. Estos objetivos han quedado incorporados a la agenda digital española, aprobada por el Gobierno en febrero de 2013.

Para ello, según estimaciones de la Comisión Europea, se deberá invertir hasta dicha fecha una cantidad comprendida entre los 180.000 y 270.000 millones de euros. Se calcula que en España serán necesarias inversiones del sector privado por valor de 23.000 millones de euros.

Estas inversiones pueden tener un gran impacto económico y social. La Comisión Europea estima que, por cada aumento de la penetración de la banda ancha en un 10 %, la economía (PIB) crece entre el 1% y el 1,5%. A su vez, la OCDE considera que un incremento del 10% de penetración de banda ancha en cualquier año implica un incremento del 1,5% de la productividad durante los siguientes 5 años.

Asimismo, como ha señalado la Comisión Europea, el despliegue de redes ultrarrápidas puede tener un importante impacto en la creación de empleo, estimándose que la innovación podría generar 2 millones de empleos para 2020, incluidos trabajos en sectores relacionados, como la provisión de contenidos o la fabricación de equipos.

Por otra parte, además de estimular la inversión, es necesario continuar promoviendo y velando por la competencia efectiva en el sector de las telecomunicaciones. Debe tenerse en cuenta en este sentido que el continuo proceso de innovación tecnológica presente en este sector exige grandes inversiones en el despliegue de redes o infraestructuras y en la comercialización de servicios que generan igualmente barreras de entrada en el sector, dificultando en consecuencia la competencia. Esta Ley persigue como objetivo fomentar la competencia sin desincentivar las inversiones.

En consecuencia, introduce reformas estructurales en el régimen jurídico de las telecomunicaciones dirigidas a facilitar el despliegue de redes y la prestación de servicios por parte de los operadores, para que ello les permita ofrecer a los usuarios servicios más innovadores, de mayor calidad y cobertura, a precios más competitivos y con mejores condiciones, lo que contribuirá a potenciar la competitividad y la productividad de la economía española en su conjunto. También favorece la seguridad jurídica, al compendiar la normativa vigente, y en particular en lo que se refiere al marco comunitario de las comunicaciones electrónicas.

Pero al mismo tiempo, y en la medida en que la existencia de competencia efectiva constituye un mecanismo eficaz de presión sobre los precios, así como sobre la calidad de los servicios y la innovación, la Ley contempla un conjunto de obligaciones o medidas que podrán imponerse ex ante a los operadores con poder significativo en el mercado. No obstante, será igualmente decisiva la labor ex post de la Comisión Nacional de los Mercados y la Competencia en la persecución de las prácticas restrictivas de la competencia, tanto de conductas colusorias, como de abusos de posición de dominio, que puedan afectar a este

sector. Es por tanto esencial que esta Comisión lleve a cabo una continua supervisión de los distintos mercados de comunicaciones electrónicas para garantizar, preservar y promover una competencia efectiva en ellos que proporcione finalmente beneficios a los usuarios.

III

La presente Ley persigue, por tanto, garantizar el cumplimiento de los objetivos de la Agenda Digital para Europa, que requiere, en la actual situación de evolución tecnológica e incertidumbre económica, asegurar un marco regulatorio claro y estable que fomente la inversión, proporcione seguridad jurídica y elimine las barreras que han dificultado el despliegue de redes, y un mayor grado de competencia en el mercado.

Para ello, con fundamento en la competencia exclusiva estatal en materia de telecomunicaciones del artículo 149.1.21.ª de la Constitución y en las competencias de carácter transversal de los artículos 149.1.1.ª y 149.1.13.ª del texto constitucional, la Ley persigue, como uno de sus principales objetivos, el de recuperar la unidad de mercado en el sector de las telecomunicaciones, estableciendo procedimientos de coordinación y resolución de conflictos entre la legislación sectorial estatal y la legislación de las Administraciones competentes dictada en el ejercicio de sus competencias que pueda afectar al despliegue de redes y a la prestación de servicios.

Con el mismo objetivo de facilitar el despliegue de redes y la prestación de servicios de comunicaciones electrónicas, se procede a una simplificación administrativa, eliminando licencias y autorizaciones por parte de la administración de las telecomunicaciones para determinadas categorías de instalaciones que hacen uso del espectro. En la misma línea se prevé una revisión de las licencias o autorizaciones por parte de las Administraciones competentes, eliminando su exigibilidad para determinadas instalaciones en propiedad privada o para la renovación tecnológica de las redes y se facilita el despliegue de las nuevas redes permitiendo el acceso a las infraestructuras de otros sectores económicos susceptibles de ser utilizadas para el despliegue de redes de comunicaciones electrónicas.

En esta misma línea de reducción de cargas administrativas, la Ley simplifica las obligaciones de información de los operadores, a los que únicamente se les podrá solicitar aquella información que no se encuentre ya en poder de las Autoridades Nacionales de Reglamentación.

Asimismo, se establecen condiciones estrictas para la existencia de operadores controlados directa o indirectamente por administraciones públicas, de manera que, fuera del concepto de autoprestación, se garantice la provisión de los servicios bajo condiciones de mercado y criterios de inversor privado, evitando de este modo que se produzcan distorsiones de la competencia, y con el objetivo de racionalizar el gasto público.

La Ley incorpora, asimismo, las previsiones recogidas en la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y de la Competencia, atribuyendo en todo caso a dicha Comisión las competencias de regulación ex ante y resolución de conflictos entre operadores reconocidas por la normativa comunitaria.

Por último, como necesario contrapunto a la reducción de las cargas y obligaciones impuestas a los operadores, la Ley refuerza el control del dominio público radioeléctrico y las potestades de inspección y sanción, facilitando la adopción de medidas cautelares y revisando la cuantía de las sanciones.

En definitiva, los criterios de liberalización del sector, libre competencia, de recuperación de la unidad de mercado y de reducción de cargas que inspiran este texto legal pretenden aportar seguridad jurídica a los operadores y crear las condiciones necesarias para la existencia de una competencia efectiva, para la realización de inversiones en el despliegue de redes de nueva generación y para la prestación de nuevos servicios, de modo que el sector pueda contribuir al necesario crecimiento económico del país.

IV

La Ley consta de ochenta y cuatro artículos agrupados en ocho títulos, diecinueve disposiciones adicionales, doce disposiciones transitorias, una disposición derogatoria, once disposiciones finales y dos anexos.

El Título I, «Disposiciones generales», establece, entre otras cuestiones, el objeto de la Ley, que no se limita a la regulación de las «comunicaciones electrónicas», término que, de acuerdo con las Directivas comunitarias, engloba aspectos tales como la habilitación para actuar como operador, los derechos y obligaciones de operadores y usuarios, o el servicio universal, sino que aborda, de forma integral, el régimen de las «telecomunicaciones» al que se refiere el artículo 149.1.21.ª de la Constitución Española. Por ello, la presente Ley regula, asimismo, otras cuestiones como la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos y aparatos, temas que a nivel comunitario son objeto de normativa específica.

La Ley excluye expresamente de su regulación los contenidos difundidos a través de servicios de comunicación audiovisual, que constituyen parte del régimen de los medios de comunicación social, y que se caracterizan por ser transmitidos en un solo sentido de forma simultánea a una multiplicidad de usuarios. No obstante, las redes utilizadas como soporte de los servicios de radiodifusión sonora y televisiva y los recursos asociados sí son parte integrante de las comunicaciones electrónicas reguladas en la presente Ley.

Igualmente se excluye de su regulación la prestación de servicios sobre las redes de telecomunicaciones que no consistan principalmente en el transporte de señales a través de dichas redes. Estos últimos son objeto de regulación en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, en este Título, se reordenan los objetivos y principios de la Ley, ya recogidos en la regulación anterior, incidiendo en la importancia de alcanzar un equilibrio entre el fomento de la innovación, el despliegue de nuevas redes, la prestación de nuevos servicios y la garantía de una competencia efectiva en los mercados de telecomunicaciones.

El Título II de la Ley, relativo al régimen general de explotación de redes y prestación de servicios, refleja la plena liberalización del sector.

De acuerdo con los principios de necesidad y proporcionalidad, la habilitación para la prestación y explotación de redes viene concedida con carácter general e inmediato por la Ley con el único requisito de notificación al Registro de Operadores, que ahora pasa a encuadrarse en el Ministerio de Industria, Energía y Turismo.

Asimismo, deberán de ser objeto de notificación los casos de autoprestación por operadores controlados directa o indirectamente por administraciones públicas. La Ley establece limitaciones concretas para la instalación y explotación de redes y la prestación de servicios por las administraciones públicas, para evitar distorsiones a la competencia que puedan derivarse de la participación de operadores públicos en el mercado de comunicaciones electrónicas.

De acuerdo con las Directivas de la Unión Europea, la Ley se refiere a las funciones de la Comisión Nacional de los Mercados y de la Competencia, que en su calidad de autoridad nacional de regulación independiente, en todo caso ejercerá aquellas relacionadas con la imposición de regulación ex ante en el marco de los procesos de análisis de mercados, con la resolución de conflictos entre operadores y con la posible imposición de la obligación de separación funcional, regulando las obligaciones aplicables a los operadores con poder significativo en mercados de referencia.

Asimismo, se han recogido determinadas previsiones en el Título II de esta Ley, al objeto de garantizar que los mercados de comunicaciones electrónicas se desarrollen en un entorno de competencia efectiva. A estos efectos, es necesario asegurar que los procesos de análisis de mercados para la imposición, en su caso, de obligaciones específicas en el marco de la regulación ex ante, se acometan con la debida periodicidad. De la misma manera, y con el fin de reprimir prácticas restrictivas de la competencia, la Comisión Nacional de los Mercados y la Competencia supervisará el funcionamiento de los distintos mercados de comunicaciones electrónicas, así como a los distintos operadores que desarrollan su actividad en ellos.

El Título III de la Ley, relativo a obligaciones y derechos de operadores y usuarios, incluye los preceptos relativos al servicio universal, las obligaciones de integridad y seguridad de las redes y la ampliación de los derechos de los usuarios finales, y recoge importantes novedades en relación con los derechos de los operadores a la ocupación del dominio público y privado, al despliegue de redes y al acceso a infraestructuras de otros sectores.

En el ámbito de la simplificación administrativa, es necesario recordar que en la Ley 12/2012, de 26 de diciembre, de medidas urgentes de liberalización del comercio y de determinados servicios, se han sustituido determinadas licencias para el despliegue de determinadas redes de telecomunicaciones en dominio privado por una declaración responsable.

En la presente Ley se establece que para el resto de actuaciones de despliegue de redes en dominio privado se puedan sustituir igualmente las licencias por una declaración responsable en aquellos casos en los que previamente el operador haya presentado ante las administraciones competentes un plan de despliegue y éste haya sido aprobado, por cuanto que, en estos casos, la administración competente ya ha analizado y ponderado los intereses inherentes al ejercicio de sus propias competencias. Las actuaciones que impliquen una mera actualización tecnológica sin afectar a elementos de obra civil o mástiles no requerirán autorización.

Con el objetivo de garantizar la unidad de mercado, facilitar la instalación y despliegue de redes y la prestación de nuevos servicios, la Ley incorpora los mecanismos necesarios de cooperación y resolución de conflictos. Los instrumentos de planeamiento territorial o urbanístico elaborados por las administraciones públicas competentes que puedan afectar al despliegue de redes serán objeto de informe del Ministerio de Industria, Energía y Turismo, previéndose cuando sea necesario un procedimiento de negociación entre el Ministerio de Industria, Energía y Turismo y los órganos encargados de la aprobación, modificación o revisión de dichos instrumentos de planificación.

Por último, se contempla la necesaria previsión de infraestructuras de comunicaciones electrónicas en zonas de urbanización y se garantiza el derecho de acceso de los operadores a infraestructuras de administraciones públicas y a infraestructuras lineales como electricidad, gas, agua, saneamiento o transporte. Estas medidas se encuentran alineadas con las propuestas realizadas por la Comisión Europea en su documento de 27 de abril de 2012 relativo a las medidas para reducir los costes del despliegue de las redes de muy alta velocidad en Europa.

Con el objetivo de reforzar los derechos de los usuarios, se clarifican los derechos introducidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones por el real decreto-Ley 13/2012, de 30 de marzo. Es destacable la mejor identificación de los derechos de los usuarios de telecomunicaciones relacionados con la protección de datos de carácter personal y la privacidad de las personas, y el mantenimiento del procedimiento extrajudicial de resolución de controversias entre operadores y usuarios finales ante el Ministerio de Industria, Energía y Turismo. Asimismo se prevé que la normativa específica sectorial establecida en la presente Ley prevalecerá sobre la normativa general de defensa de los consumidores y usuarios, tal y como queda recogido en la propia normativa comunitaria, en particular en el apartado 2 del artículo 3 de la Directiva 2011/83/UE de 25 de octubre de 2011 sobre los derechos de los consumidores.

En el Título IV, relativo a la evaluación de la conformidad de equipos y aparatos, se regulan, entre otros, aspectos tales como la normalización técnica, la evaluación de la conformidad de equipos y aparatos, y las condiciones que deben cumplir las instalaciones.

En relación con la administración del dominio público radioeléctrico, el Título V procede a una clarificación de los principios aplicables, de las actuaciones que abarca dicha administración, de los tipos de uso y de los distintos títulos habilitantes, introduce una simplificación administrativa para el acceso a determinadas bandas de frecuencia, y consolida las últimas reformas en materia de duración, modificación, extinción y revocación de títulos y en relación al mercado secundario del espectro. Como novedad, se introducen medidas destinadas a evitar el uso del espectro por quienes no disponen de título habilitante para ello, garantizando con ello la disponibilidad y uso eficiente de este recurso escaso, en particular mediante su protección activa y la colaboración de los operadores de red.

El Título VI, «La administración de las telecomunicaciones» determina las competencias que tienen atribuidas las diferentes Autoridades Nacionales de Reglamentación. Concretamente, este título incorpora el reparto competencial que inspira la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y de la Competencia, atribuyendo a dicha Comisión funciones como la definición y análisis de los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas, la identificación del

operador u operadores con poder significativo de mercado, el establecimiento, si procede, de obligaciones específicas a dichos operadores, la resolución de conflictos en los mercados de comunicaciones electrónicas o la determinación del coste neto en la prestación del servicio universal, entre otras.

En el Título VII, «Tasas en materia de telecomunicaciones» y en el Anexo I, la Ley introduce importantes mejoras respecto de la regulación contenida en la Ley 32/2003, de 3 de noviembre, en materia de tasas de telecomunicaciones. En particular, se reduce el límite máximo de la tasa general de operadores dirigida a financiar los costes en que incurren las Autoridades Nacionales de Reglamentación por la aplicación del régimen jurídico establecido en esta Ley y se establece un esquema de ajuste automático a los costes a los que han tenido que hacer frente las Autoridades Nacionales de Reglamentación.

El Título VIII relativo a inspección y régimen sancionador refuerza las potestades inspectoras, exigiendo la colaboración de los titulares de fincas o inmuebles en los que se ubiquen instalaciones de telecomunicaciones para la identificación de los titulares de dichas instalaciones, mejora la tipificación de infracciones, revisa la clasificación y cuantía de las sanciones, proporciona criterios para la determinación de la cuantía de la sanción, y facilita la adopción de medidas cautelares que podrán acordarse incluso antes de iniciar el expediente sancionador.

Las disposiciones adicionales regulan, entre otras cuestiones, el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, las obligaciones en materia de acceso condicional, acceso a determinados servicios de radiodifusión y televisión, televisión de formato ancho y obligaciones de transmisión, así como la creación de la Comisión Interministerial sobre radiofrecuencias y salud encargada de informar sobre las medidas aprobadas en materia de protección sanitaria frente a emisiones radioeléctricas y de los múltiples controles a que son sometidas las instalaciones generadoras de dichas emisiones.

En particular, una de las disposiciones adicionales persigue la universalización de la banda ancha ultrarrápida, en virtud de la cual el Gobierno establecerá una Estrategia Nacional de Redes Ultrarrápidas que tenga como objetivo impulsar el despliegue de redes de acceso ultrarrápido a la banda ancha, tanto fijo como móvil, de cara a lograr su universalización, así como fomentar su adopción por ciudadanos, empresas y administraciones, para garantizar la cohesión social y territorial en colaboración con las administraciones territoriales.

En la ejecución de esta Estrategia se podrán incluir medidas como la realización anual de convocatorias públicas de ayudas para la extensión de la cobertura de la banda ancha ultrarrápida que, bajo el principio de neutralidad tecnológica, doten de cobertura a zonas en las que no existe oferta y en las que no esté prevista en el corto plazo, en particular, con el objetivo de permitir acortar plazos de conexión y abaratar costes en núcleos rurales de difícil orografía y baja densidad de población. Estas convocatorias públicas garantizarán que las ayudas cubrirán sólo un porcentaje de la inversión, que las ayudas se adjudicarán en régimen de concurrencia competitiva, y que la necesidad de la ayuda se encuentra justificada en la existencia de un déficit comercial a corto o medio plazo que impide la ejecución del proyecto dada su baja rentabilidad, y contemple mecanismos para evitar una posible sobre compensación.

Asimismo, se establecerán zonas de actuación preferente en base a las mayores necesidades de los usuarios, de su carácter dinamizador, del grado de presencia de PYMES o de centros de actividad económica como polígonos industriales o centros turísticos y de otros factores como el equilibrio territorial, su mayor incidencia sobre el desarrollo económico, su alejamiento, o la disponibilidad de financiación con cargo al Fondo Europeo de Desarrollo Regional (FEDER).

Dicha Estrategia se complementará con otras medidas contempladas en la presente Ley orientadas a facilitar el despliegue de redes ultrarrápidas de acceso fijo y móvil, y facilitar la modernización y renovación de las redes.

Por su parte, las disposiciones transitorias regulan diferentes aspectos que facilitarán la transición hacia la aplicación de esta nueva Ley, como la adaptación de los operadores controlados directa o indirectamente por administraciones públicas al régimen previsto en el artículo 9 o el régimen transitorio para la fijación de las tasas recogidas en el Anexo I.

Por último, en las disposiciones finales, la Ley modifica diversos textos normativos. En particular, se modifican diversos preceptos de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, a fin de adaptarla al marco social y económico actual. En concreto, se introducen precisiones sobre el consentimiento del destinatario para aceptar el tratamiento de los datos derivado de dispositivos de almacenamiento y recuperación de datos en sus equipos terminales, y se establecen criterios para la modulación de las sanciones.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación de la Ley.*

1. El ámbito de aplicación de esta Ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados, de conformidad con el artículo 149.1.21.ª de la Constitución.

2. Quedan excluidos del ámbito de esta Ley los servicios de comunicación audiovisual, los contenidos audiovisuales transmitidos a través de las redes, así como el régimen básico de los medios de comunicación social de naturaleza audiovisual a que se refiere el artículo 149.1.27.ª de la Constitución.

Asimismo, se excluyen del ámbito de esta Ley los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas, las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos y los servicios de la Sociedad de la Información, regulados en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.

Artículo 2. *Las telecomunicaciones como servicios de interés general.*

1. Las telecomunicaciones son servicios de interés general que se prestan en régimen de libre competencia.

2. Sólo tienen la consideración de servicio público o están sometidos a obligaciones de servicio público los servicios regulados en el artículo 4 y en el Título III de esta Ley.

La imposición de obligaciones de servicio público perseguirá la consecución de los objetivos establecidos en el artículo 3 de esta Ley y podrá recaer sobre los operadores que obtengan derechos de ocupación del dominio público o de la propiedad privada, de derechos de uso del dominio público radioeléctrico, de derechos de uso de recursos públicos de numeración, direccionamiento o de denominación o que ostenten la condición de operador con poder significativo en un determinado mercado de referencia.

Artículo 3. *Objetivos y principios de la Ley.*

Los objetivos y principios de esta Ley son los siguientes:

a) Fomentar la competencia efectiva en los mercados de telecomunicaciones para potenciar al máximo los beneficios para las empresas y los consumidores, principalmente en términos de bajada de los precios, calidad de los servicios e innovación, teniendo debidamente en cuenta la variedad de condiciones en cuanto a la competencia y los consumidores que existen en las distintas áreas geográficas, y velando por que no exista falseamiento ni restricción de la competencia en la explotación de redes o en la prestación de servicios de comunicaciones electrónicas, incluida la transmisión de contenidos.

b) Desarrollar la economía y el empleo digital, promover el desarrollo del sector de las telecomunicaciones y de todos los nuevos servicios digitales que las nuevas redes ultrarrápidas permiten, impulsando la cohesión social y territorial, mediante la mejora y extensión de las redes, así como la prestación de los servicios de comunicaciones electrónicas y el suministro de los recursos asociados a ellas.

c) Promover el despliegue de redes y la prestación de servicios de comunicaciones electrónicas, fomentando la conectividad y la interoperabilidad extremo a extremo y su acceso, en condiciones de igualdad y no discriminación.

d) Promover el desarrollo de la industria de productos y equipos de telecomunicaciones.

e) Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

f) Promover la inversión eficiente en materia de infraestructuras incluyendo, cuando proceda, la competencia basada en infraestructuras, fomentando la innovación y teniendo debidamente en cuenta los riesgos en que incurren las empresas inversoras.

g) Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones, como la numeración y el espectro radioeléctrico, y la adecuada protección de este último, y el acceso a los derechos de ocupación de la propiedad pública y privada.

h) Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.

i) Garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas a las que se refiere el Título III, en especial las de servicio universal.

j) Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en condiciones adecuadas de elección, precio y buena calidad, promoviendo la capacidad de los usuarios finales para acceder y distribuir la información o utilizar las aplicaciones y los servicios de su elección, en particular a través de un acceso abierto a Internet. En la prestación de estos servicios deben salvaguardarse los imperativos constitucionales de no discriminación, de respeto a los derechos al honor y a la intimidad, la protección a la juventud y a la infancia, la protección de los datos personales y el secreto en las comunicaciones.

k) Salvaguardar y proteger en los mercados de telecomunicaciones la satisfacción de las necesidades de grupos sociales específicos, las personas con discapacidad, las personas mayores, las personas en situación de dependencia y usuarios con necesidades sociales especiales, atendiendo a los principios de igualdad de oportunidades y no discriminación. En lo relativo al acceso a los servicios de comunicaciones electrónicas de las personas en situación de dependencia, se fomentará el cumplimiento de las normas o las especificaciones pertinentes relativas a normalización técnica publicadas de acuerdo con la normativa comunitaria.

l) Facilitar el acceso de los usuarios con discapacidad a los servicios de comunicaciones electrónicas y al uso de equipos terminales.

Artículo 4. *Servicios de telecomunicaciones para la defensa nacional, la seguridad pública, la seguridad vial y la protección civil.*

1. Sólo tienen la consideración de servicio público los servicios regulados en este artículo.

2. Las redes, servicios, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la defensa nacional integran los medios destinados a ésta, se reservan al Estado y se rigen por su normativa específica.

3. El Ministerio de Industria, Energía y Turismo es el órgano de la Administración General del Estado con competencia, de conformidad con la legislación específica sobre la materia y lo establecido en esta Ley, para ejecutar, en la medida en que le afecte, la política de defensa nacional en el sector de las telecomunicaciones, con la debida coordinación con el Ministerio de Defensa y siguiendo los criterios fijados por éste.

En el marco de las funciones relacionadas con la defensa civil, corresponde al Ministerio de Industria, Energía y Turismo estudiar, planear, programar, proponer y ejecutar cuantas medidas se relacionen con su aportación a la defensa nacional en el ámbito de las telecomunicaciones.

A tales efectos, los Ministerios de Defensa y de Industria, Energía y Turismo coordinarán la planificación del sistema de telecomunicaciones de las Fuerzas Armadas, a fin de asegurar, en la medida de lo posible, su compatibilidad con los servicios civiles. Asimismo elaborarán los programas de coordinación tecnológica precisos que faciliten la armonización, homologación y utilización, conjunta o indistinta, de los medios, sistemas y redes civiles y militares en el ámbito de las telecomunicaciones. Para el estudio e informe de estas

materias, se constituirán los órganos interministeriales que se consideren adecuados, con la composición y competencia que se determinen mediante real decreto.

4. En los ámbitos de la seguridad pública, seguridad vial y de la protección civil, en su específica relación con el uso de las telecomunicaciones, el Ministerio de Industria, Energía y Turismo cooperará con el Ministerio del Interior y con los órganos responsables de las comunidades autónomas con competencias sobre las citadas materias.

5. Los bienes muebles o inmuebles vinculados a los centros, establecimientos y dependencias afectos a la explotación de las redes y a la prestación de los servicios de telecomunicaciones dispondrán de las medidas y sistemas de seguridad, vigilancia, difusión de información, prevención de riesgos y protección que se determinen por el Gobierno, a propuesta de los Ministerios de Defensa, del Interior o de Industria, Energía y Turismo, dentro del ámbito de sus respectivas competencias. Estas medidas y sistemas deberán estar disponibles en las situaciones de normalidad o en las de crisis, así como en los supuestos contemplados en la Ley Orgánica 4/1981, de 1 de junio, reguladora de los Estados de Alarma, Excepción y Sitio, y en la Ley 2/1985, de 21 de enero, de Protección Civil.

6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de determinados servicios o de la explotación de ciertas redes de comunicaciones electrónicas, de acuerdo con el texto refundido de la Ley de Contratos del Sector Público, aprobado por el real decreto Legislativo 3/2011, de 14 de noviembre, para garantizar la seguridad pública y la defensa nacional. Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de los correspondientes servicios o de la explotación de las correspondientes redes. En este último caso, podrá, con las mismas condiciones, intervenir la prestación de los servicios de comunicaciones electrónicas.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de éste o los de intervenir o explotar las redes a los que se refiere el párrafo anterior se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración pública competente. En este último caso será preciso que la Administración pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquélla tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.

7. La regulación contenida en esta Ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional.

TÍTULO II

Explotación de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia

CAPÍTULO I

Disposiciones generales

Artículo 5. *Principios aplicables.*

1. La explotación de las redes y la prestación de los servicios de comunicaciones electrónicas se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta Ley y su normativa de desarrollo.

2. La adquisición de los derechos de uso del dominio público radioeléctrico, de ocupación del dominio público o de la propiedad privada y de los recursos de numeración, direccionamiento y denominación necesarios para la explotación de redes y para la

prestación de servicios de comunicaciones electrónicas deberá realizarse conforme a lo dispuesto en esta Ley y en lo no contemplado en la misma por su normativa específica.

3. Las medidas que se adopten en relación al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas respetarán los derechos y libertades fundamentales, como queda garantizado en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, en los principios generales del Derecho comunitario y en la Constitución Española.

Cualquiera de esas medidas relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de restringir esos derechos y libertades fundamentales solo podrá imponerse si es adecuada, proporcionada y necesaria en una sociedad democrática, y su aplicación estará sujeta a las salvaguardias de procedimiento apropiadas de conformidad con las normas mencionadas en el párrafo anterior. Por tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia y el derecho a la vida privada, a través de un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los arreglos procesales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. Asimismo, se garantizará el derecho a la tutela judicial efectiva y en tiempo oportuno.

Artículo 6. *Requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas.*

1. Podrán explotar redes y prestar servicios de comunicaciones electrónicas a terceros las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o de otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

2. Los interesados en la explotación de una determinada red o en la prestación de un determinado servicio de comunicaciones electrónicas deberán, con anterioridad al inicio de la actividad, comunicarlo previamente al Registro de operadores en los términos que se determinen mediante real decreto, sometiéndose a las condiciones previstas para el ejercicio de la actividad que pretendan realizar.

Sin perjuicio de lo dispuesto para los operadores controlados directa o indirectamente por administraciones públicas en el artículo 7, quedan exentos de esta obligación quienes exploten redes y presten servicios de comunicaciones electrónicas en régimen de autoprestación.

Artículo 7. *Registro de operadores.*

1. Se crea, dependiente del Ministerio de Industria, Energía y Turismo, el Registro de operadores. Dicho Registro será de carácter público y su regulación se hará por real decreto. Se garantizará que el acceso a dicho Registro pueda efectuarse por medios electrónicos. En él deberán inscribirse los datos relativos a las personas físicas o jurídicas que hayan notificado su intención de explotar redes o prestar servicios de comunicaciones electrónicas, las condiciones para desarrollar la actividad y sus modificaciones.

2. Cuando el Registro de operadores constate que la notificación a que se refiere el apartado 2 del artículo anterior no reúne los requisitos establecidos dictará resolución motivada en un plazo máximo de 15 días hábiles, no teniendo por realizada aquélla.

3. Las administraciones públicas deberán comunicar al Registro de operadores todo proyecto de instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público, tanto si dicha instalación o explotación vaya a realizarse de manera directa o a través de cualquier entidad o sociedad. Mediante real decreto podrán especificarse aquellos supuestos en que, en atención a las características, la dimensión de la red proyectada o la naturaleza de los servicios a prestar, no resulte necesario efectuar dicha comunicación.

4. Quienes resultasen seleccionados para la prestación de servicios de comunicaciones electrónicas armonizados en procedimientos de licitación convocados por las instituciones de la Unión Europea serán inscritos de oficio en el Registro de operadores.

5. No será preciso el consentimiento del interesado para el tratamiento de los datos de carácter personal que haya de contener el Registro ni para la comunicación de dichos datos que se derive de su publicidad.

Artículo 8. *Condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas.*

1. La explotación de las redes y la prestación de los servicios de comunicaciones electrónicas se sujetarán a las condiciones previstas en esta Ley y su normativa de desarrollo, entre las cuales se incluirán las de salvaguarda de los derechos de los usuarios finales.

2. Con arreglo a los principios de objetividad y de proporcionalidad, el Gobierno podrá modificar las condiciones impuestas previa audiencia de los interesados, del Consejo de Consumidores y Usuarios y, en su caso, de las asociaciones más representativas de los restantes usuarios, e informe de la Comisión Nacional de los Mercados y de la Competencia. La modificación se realizará mediante real decreto, en el que deberá constar la justificación en que se sustenta y establecerá un plazo para que los operadores se adapten a aquélla.

3. Las entidades públicas o privadas que, de acuerdo con la legislación vigente, tengan derechos especiales o exclusivos para la prestación de servicios en otro sector económico y que exploten redes públicas o presten servicios de comunicaciones electrónicas disponibles al público deberán llevar cuentas separadas y auditadas para sus actividades de comunicaciones electrónicas, o establecer una separación estructural para las actividades asociadas con la explotación de redes o la prestación de servicios de comunicaciones electrónicas. Mediante real decreto podrá establecerse la exención de esta obligación para las entidades cuyos ingresos brutos de explotación anuales por actividades asociadas con las redes o servicios de comunicaciones electrónicas sea inferior a 50 millones de euros.

Artículo 9. *Instalación y explotación de redes públicas y prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por las administraciones públicas.*

1. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por operadores controlados directa o indirectamente por administraciones públicas se regirá de manera específica por lo dispuesto en el presente artículo.

2. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por operadores controlados directa o indirectamente por administraciones públicas se realizará dando cumplimiento al principio de inversor privado, con la debida separación de cuentas, con arreglo a los principios de neutralidad, transparencia, no distorsión de la competencia y no discriminación, y cumpliendo con la normativa sobre ayudas de Estado a que se refieren los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea.

Mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se determinarán las condiciones en que los operadores controlados directa o indirectamente por administraciones públicas deberán llevar a cabo la instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros y, en especial, los criterios, condiciones y requisitos para que dichos operadores actúen con sujeción al principio de inversor privado. En particular, en dicho real decreto se establecerán los supuestos en los que, como excepción a la exigencia de actuación con sujeción al principio de inversor privado, los operadores controlados directa o indirectamente por administraciones públicas podrán instalar y explotar redes públicas y prestar servicios de comunicaciones electrónicas en régimen de prestación a terceros que no distorsionen la competencia o cuando se confirme fallo del mercado y no exista interés de concurrencia en el despliegue del sector privado por ausencia o insuficiencia de inversión privada, ajustándose la inversión pública al principio de necesidad, con la finalidad de garantizar la necesaria cohesión territorial y social.

3. Una Administración Pública sólo podrá instalar y explotar redes públicas de comunicaciones electrónicas o prestar servicios de comunicaciones electrónicas en régimen de prestación a terceros a través de entidades o sociedades que tengan entre su objeto social o finalidad la instalación y explotación de redes o la prestación de servicios de comunicaciones electrónicas.

La instalación o explotación de redes públicas de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por los órganos o entes gestores de infraestructuras de transporte de competencia estatal, se realizará en las condiciones establecidas en el artículo 38 de la presente Ley.

4. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por operadores controlados directa o indirectamente por administraciones públicas deberán llevarse a cabo en las condiciones establecidas en el artículo 8 y, en particular, en las siguientes condiciones:

a) Los operadores tienen reconocido directamente el derecho a acceder en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias a las infraestructuras y recursos asociados utilizados por los operadores controlados directa o indirectamente por administraciones públicas para la instalación y explotación de redes de comunicaciones electrónicas.

b) Los operadores tienen reconocido directamente el derecho de uso compartido de las infraestructuras de red de comunicaciones electrónicas y sus recursos asociados instaladas por los operadores controlados directa o indirectamente por administraciones públicas en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias.

c) Si las administraciones públicas reguladoras o titulares del dominio público ostentan la propiedad, total o parcial, o ejercen el control directo o indirecto de operadores que explotan redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, deberán mantener una separación estructural entre dichos operadores y los órganos encargados de la regulación y gestión de los derechos de utilización del dominio público correspondiente.

Artículo 10. *Obligaciones de suministro de información.*

1. Las Autoridades Nacionales de Reglamentación de Telecomunicaciones podrán, en el ámbito de su actuación, requerir a las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas, así como a aquellos otros agentes que intervengan en este mercado, la información necesaria para el cumplimiento de alguna de las siguientes finalidades:

a) Satisfacer necesidades estadísticas o de análisis y para la elaboración de informes de seguimiento sectoriales.

b) Comprobar el cumplimiento de las condiciones establecidas para la prestación de servicios o la explotación de redes de comunicaciones electrónicas, en particular, cuando la explotación de las redes conlleve emisiones radioeléctricas.

c) Comprobar que la prestación de servicios o la explotación de redes de comunicaciones electrónicas por parte de operadores controlados directa o indirectamente por administraciones públicas cumplen las condiciones establecidas por esta Ley y sus normas de desarrollo.

d) Evaluar la procedencia de las solicitudes de derechos de uso del dominio público radioeléctrico y de la numeración.

e) Comprobar el uso efectivo y eficiente de frecuencias y números y el cumplimiento de las obligaciones que resulten de los derechos de uso del dominio público radioeléctrico, de la numeración, direccionamiento y denominación o de la ocupación del dominio público o de la propiedad privada.

f) Elaborar análisis que permitan la definición de los mercados de referencia, el establecimiento de condiciones específicas a los operadores con poder significativo de mercado en aquéllos y conocer el modo en que la futura evolución de las redes o los servicios puede repercutir en los servicios mayoristas que las empresas ponen a disposición de sus competidores. Asimismo, podrá exigirse a las empresas con un poder significativo en

los mercados mayoristas que presenten datos contables sobre los mercados minoristas asociados con dichos mercados mayoristas.

g) Comprobar el cumplimiento de las obligaciones específicas impuestas en el marco de la regulación ex ante y el cumplimiento de las resoluciones dictadas para resolver conflictos entre operadores.

h) Comprobar el cumplimiento de las obligaciones de servicio público y obligaciones de carácter público, así como determinar los operadores encargados de prestar el servicio universal.

i) Comprobar el cumplimiento de las obligaciones que resulten necesarias para garantizar un acceso equivalente para los usuarios finales con discapacidad y que éstos se beneficien de la posibilidad de elección de empresas y servicios disponibles para la mayoría de los usuarios finales.

j) La puesta a disposición de los ciudadanos de información o aplicaciones interactivas que posibiliten realizar comparativas sobre precios, cobertura y calidad de los servicios, en interés de los usuarios.

k) La adopción de medidas destinadas a facilitar la coubicación o el uso compartido de elementos de redes públicas de comunicaciones electrónicas y recursos asociados.

l) Evaluar la integridad y la seguridad de las redes y servicios de comunicaciones electrónicas.

m) Cumplir los requerimientos que vengan impuestos en el ordenamiento jurídico.

n) Comprobar el cumplimiento del resto de obligaciones nacidas de esta Ley.

o) Planificar de manera eficiente el uso de fondos públicos destinados, en su caso, al despliegue de infraestructuras de telecomunicaciones.

Esta información, excepto aquella a la que se refieren los párrafos d) y o), no podrá exigirse antes del inicio de la actividad y se suministrará en el plazo y forma que se establezca en cada requerimiento, atendidas las circunstancias del caso. Las Autoridades Nacionales de Reglamentación garantizarán la confidencialidad de la información suministrada que pueda afectar a la seguridad e integridad de las redes y de los servicios de comunicaciones electrónicas o al secreto comercial o industrial.

2. Las administraciones públicas podrán solicitar la información que sea necesaria en el ejercicio de sus competencias.

Las administraciones públicas, antes de solicitar información en materia de telecomunicaciones a las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas para el ejercicio de sus funciones, deberán recabar dicha información de las Autoridades Nacionales de Reglamentación. Únicamente en el caso de que las Autoridades Nacionales de Reglamentación no dispongan de la información solicitada o la misma no pueda ser proporcionada al ser confidencial por razones de seguridad o de secreto comercial o industrial, los órganos competentes de las administraciones públicas podrán solicitar dicha información en materia de telecomunicaciones de las personas físicas o jurídicas que exploten redes o presten servicios de comunicaciones electrónicas.

3. Las solicitudes de información que se realicen de conformidad con los apartados anteriores habrán de ser motivadas y proporcionadas al fin perseguido.

Artículo 11. *Normas técnicas.*

1. El Ministerio de Industria, Energía y Turismo fomentará el uso de las normas o especificaciones técnicas identificadas en la relación que la Comisión Europea elabore como base para fomentar la armonización del suministro de redes de comunicaciones electrónicas, servicios de comunicaciones electrónicas y recursos y servicios asociados, especialmente en los ámbitos de acceso e interconexión.

En particular, garantizará la utilización de las normas o especificaciones técnicas cuya aplicación declare obligatoria la Comisión Europea, de conformidad con lo establecido en la normativa de la Unión Europea, en la medida necesaria para garantizar la interoperabilidad de los servicios y para potenciar la libertad de elección de los usuarios.

En ausencia de dichas normas o especificaciones promoverá la aplicación de las normas o recomendaciones internacionales aprobadas por la Unión Internacional de

Telecomunicaciones (UIT), la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), la Comisión Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).

Mediante real decreto se podrán determinar las formas de elaboración y, en su caso, de adopción de las especificaciones técnicas aplicables a redes y servicios de comunicaciones electrónicas, en particular, a efectos de garantizar el cumplimiento de requisitos en materia de despliegue de redes, obligaciones de servicio público, interoperabilidad, integridad y seguridad de redes y servicios.

Mediante real decreto se establecerá el procedimiento de comunicación de las citadas especificaciones a la Comisión Europea de conformidad con la normativa de la Unión Europea.

2. La Comisión Nacional de los Mercados y la Competencia también fomentará y garantizará el uso de las normas o especificaciones técnicas en los términos señalados en el apartado anterior en el ejercicio de sus funciones de la regulación ex ante y de resolución de conflictos entre operadores.

CAPÍTULO II

Acceso a las redes y recursos asociados e interconexión

Artículo 12. *Principios generales aplicables al acceso a las redes y recursos asociados y a su interconexión.*

1. Este capítulo y su desarrollo reglamentario serán aplicables a la interconexión y a los accesos a redes públicas de comunicaciones electrónicas y a sus recursos asociados, salvo que el beneficiario del acceso sea un usuario final, de acuerdo con la definición que se da a los conceptos de acceso e interconexión en el anexo II de la presente Ley.

2. Los operadores de redes públicas de comunicaciones electrónicas tendrán el derecho y, cuando se solicite por otros operadores de redes de comunicaciones electrónicas, la obligación de negociar la interconexión mutua con el fin de prestar servicios de comunicaciones electrónicas disponibles al público, con el objeto de garantizar así la prestación de servicios y su interoperabilidad.

3. No existirán restricciones que impidan que los operadores negocien entre sí acuerdos de acceso e interconexión.

4. La persona física o jurídica habilitada para explotar redes o prestar servicios en otro Estado miembro de la Unión Europea que solicite acceso o interconexión en España no necesitará llevar a cabo la notificación a la que se refiere el artículo 6 de la Ley cuando no explote redes ni preste servicios de comunicaciones electrónicas en el territorio nacional.

5. Sin perjuicio de las medidas que puedan adoptarse en relación con las empresas que tengan un poder significativo en el mercado de acuerdo con lo previsto en el artículo 14 de esta Ley, la Comisión Nacional de los Mercados y la Competencia podrá intervenir en las relaciones entre operadores o entre operadores y otras entidades que se beneficien de las obligaciones de acceso e interconexión, a petición de cualquiera de las partes implicadas, o de oficio cuando esté justificado, con objeto de fomentar y, en su caso, garantizar la adecuación del acceso, la interconexión y la interoperabilidad de los servicios, así como la consecución de los objetivos establecidos en el artículo 3. La decisión de la Comisión Nacional de los Mercados y la Competencia será vinculante y se adoptará en el plazo indicado en la Ley 3/2013 de creación de dicha Comisión.

6. Las obligaciones y condiciones que se impongan de conformidad con este capítulo serán objetivas, transparentes, proporcionadas y no discriminatorias.

7. Los operadores que obtengan información de otros, con anterioridad, durante o con posterioridad al proceso de negociación de acuerdos de acceso o interconexión, destinarán dicha información exclusivamente a los fines para los que les fue facilitada y respetarán en todo momento la confidencialidad de la información transmitida o almacenada, en especial respecto de terceros, incluidos otros departamentos de la propia empresa, filiales o asociados.

CAPÍTULO III

Regulación ex ante de los mercados y resolución de conflictos

Artículo 13. *Mercados de referencia y operadores con poder significativo en el mercado.*

1. La Comisión Nacional de los Mercados y la Competencia, teniendo en cuenta la Recomendación de la Comisión Europea sobre mercados relevantes, las Directrices de la Comisión Europea para el análisis de mercados y determinación de operadores con poder significativo en el mercado y los dictámenes y posiciones comunes pertinentes adoptados por el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), definirá, previo informe del Ministerio de Industria, Energía y Turismo y del Ministerio de Economía y Competitividad y mediante resolución publicada en el «Boletín Oficial del Estado», los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas, entre los que se incluirán los correspondientes mercados de referencia al por mayor y al por menor, y el ámbito geográfico de los mismos, cuyas características pueden justificar la imposición de obligaciones específicas.

En todo caso, la Comisión Nacional de los Mercados y la Competencia, en aplicación de la normativa en materia de competencia, en especial, de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea, y de la Ley 3/2013, de creación de la Comisión, deberá supervisar el funcionamiento de los distintos mercados de comunicaciones electrónicas, así como la actividad de los operadores ya tengan o no poder significativo en el mercado, para preservar, garantizar y promover condiciones de competencia efectiva en los mismos.

2. Asimismo, teniendo en cuenta las referencias citadas en el párrafo anterior, la Comisión Nacional de los Mercados y la Competencia llevará a cabo un análisis de los citados mercados:

a) En un plazo máximo de tres años contado desde la adopción de una medida anterior relativa a ese mercado. No obstante, y de modo excepcional, este plazo podrá ampliarse a un máximo de tres años suplementarios cuando las autoridades nacionales de reglamentación hayan notificado una propuesta de ampliación razonada a la Comisión Europea y esta no haya hecho ninguna objeción en el plazo de un mes respecto de la ampliación notificada.

b) En el plazo máximo de dos años desde la adopción de una recomendación sobre mercados relevantes revisada, para los mercados no notificados previamente a la Comisión Europea.

Si la Comisión Nacional de los Mercados y la Competencia no hubiera concluido su análisis de un mercado relevante que figura en la Recomendación de Mercados Relevantes dentro de los plazos establecidos, el ORECE le prestará asistencia, a petición de la propia Comisión, para la conclusión del análisis del mercado concreto y la determinación de las obligaciones específicas que deban imponerse. La Comisión Nacional de los Mercados y la Competencia, contando con esta colaboración, notificará el proyecto de medida a la Comisión Europea en un plazo de seis meses.

El Ministerio de Industria, Energía y Turismo, en virtud de lo dispuesto en el artículo 5.2 de la Ley 3/2013, podrá solicitar a la Comisión Nacional de los Mercados y la Competencia para que realice el análisis de un mercado determinado de comunicaciones electrónicas cuando concurran razones de interés general, o bien se aprecien indicios de falta de competencia efectiva.

La Comisión Nacional de los Mercados y la Competencia, en los planes anuales o plurianuales de actuación que apruebe y en los que debe constar sus objetivos y prioridades a tenor de lo dispuesto en el artículo 20.16 de la Ley 3/2013, deberá identificar los mercados relevantes que vaya a analizar y las actuaciones necesarias para la adecuada realización de dicho análisis dentro de los plazos previstos en este apartado.

El Presidente de la Comisión Nacional de los Mercados y la Competencia, en el marco del control parlamentario anual a que se refiere el artículo 39.1 de la Ley 3/2013, deberá dar

cuenta del resultado de los análisis de los mercados y el cumplimiento de los plazos establecidos en este apartado.

3. El análisis a que se refiere el apartado anterior tendrá como finalidad determinar si los distintos mercados de referencia se desarrollan en un entorno de competencia efectiva. En caso contrario, la Comisión Nacional de los Mercados y la Competencia previo informe del Ministerio de Industria, Energía y Turismo y del Ministerio de Economía y Competitividad, identificará y hará públicos el operador u operadores que poseen un poder significativo en cada mercado considerado.

Cuando un operador u operadores tengan, individual o conjuntamente, poder significativo en un mercado de referencia (mercado primario), la Comisión Nacional de los Mercados y la Competencia podrá declarar que lo tienen también en otro mercado de referencia estrechamente relacionado con el anterior (mercado secundario) cuando los vínculos entre ambos sean tales que resulte posible ejercer en el mercado secundario el peso que se tiene en el mercado primario, reforzando de esta manera el poder en el mercado del operador. En este supuesto, podrán imponerse obligaciones específicas adecuadas en el mercado secundario, en virtud del apartado siguiente.

4. En aquellos mercados en que se constate la inexistencia de un entorno de competencia efectiva, la Comisión Nacional de los Mercados y la Competencia, previo informe del Ministerio de Industria, Energía y Turismo y del Ministerio de Economía y Competitividad, impondrá las obligaciones específicas apropiadas que sean exigibles a los operadores que hayan sido identificados como operadores con poder significativo en dichos mercados. Podrá a estos efectos mantener o modificar obligaciones específicas que tuvieran impuestas. En la determinación de dichas obligaciones específicas se otorgará preferencia a las medidas en mercados al por mayor frente a las actuaciones en los mercados al por menor correspondientes.

Las obligaciones específicas a que se refieren los párrafos anteriores se basarán en la naturaleza del problema identificado, serán proporcionadas y estarán justificadas en el cumplimiento de los objetivos del artículo 3 de esta Ley. Dichas obligaciones se mantendrán en vigor durante el tiempo estrictamente imprescindible.

5. En los mercados en los que se constate la existencia de competencia efectiva, la Comisión Nacional de los Mercados y la Competencia suprimirá las obligaciones específicas que, en su caso, tuvieran impuestas los operadores por haber sido declarados con poder significativo en dichos mercados.

Artículo 14. *Obligaciones específicas aplicables a los operadores con poder significativo en mercados de referencia.*

1. La Comisión Nacional de los Mercados y la Competencia, en la forma y en las condiciones que se determinen en desarrollo del apartado 5 de este artículo, podrá imponer a los operadores que, de conformidad con dicho artículo, hayan sido declarados con poder significativo en el mercado obligaciones específicas en materia de:

a) Transparencia, en relación con la interconexión y el acceso, conforme a las cuales los operadores deberán hacer público determinado tipo de información, como la relativa a contabilidad, especificaciones técnicas, características de las redes, condiciones de suministro y utilización, incluidas, en su caso, las condiciones que pudieran limitar el acceso o la utilización de servicios o aplicaciones, así como los precios. En particular, cuando de conformidad con la letra b) se impongan a un operador obligaciones de no discriminación, se le podrá exigir que publique una oferta de referencia.

Asimismo, se garantizará que los operadores a los que de conformidad con la letra d) se impongan obligaciones en relación con el acceso al por mayor a la infraestructura de la red dispongan de una oferta de referencia. Mediante real decreto se establecerá el contenido mínimo de elementos que debe contemplar dicha oferta.

b) No discriminación, que garantizarán, en particular, que el operador aplique condiciones equivalentes en circunstancias semejantes a otros operadores que presten servicios equivalentes y proporcione a terceros servicios e información de la misma calidad que los que proporcione para sus propios servicios o los de sus filiales o asociados y en las mismas condiciones.

c) Separación de cuentas, en el formato y con la metodología que, en su caso, se especifiquen.

d) Acceso a elementos o a recursos específicos de las redes y a su utilización, así como a recursos y a servicios asociados tales como servicios de identidad, localización y presencia.

e) Control de precios, tales como la fijación de precios, la orientación de los precios en función de los costes y el establecimiento de una contabilidad de costes, con objeto de garantizar la formación de precios competitivos y evitar precios excesivos y márgenes no competitivos en detrimento de los usuarios finales. La Comisión Nacional de los Mercados y la Competencia velará para que estos mecanismos de control de precios que se impongan sirvan para fomentar la competencia efectiva y los beneficios para los consumidores y usuarios en términos de precios y calidad de los servicios. Para favorecer la inversión por parte del operador, en particular en redes de próxima generación, la Comisión Nacional de los Mercados y la Competencia tendrá en cuenta la inversión efectuada, permitiendo una tasa razonable de rendimiento en relación con el capital correspondiente invertido, habida cuenta de todos los riesgos específicos de un nuevo proyecto de inversión concreto.

2. En circunstancias excepcionales y debidamente justificadas, la Comisión Nacional de los Mercados y la Competencia, previo sometimiento al mecanismo de consulta previsto en la disposición adicional octava, podrá imponer obligaciones específicas relativas al acceso o a la interconexión que no se limiten a las materias enumeradas en el apartado anterior.

3. Cuando la Comisión Nacional de los Mercados y la Competencia estudie la conveniencia de imponer las obligaciones específicas de acceso previstas en la letra d) del apartado 1 de este artículo, habrá de considerar, en particular, los siguientes elementos:

a) la viabilidad técnica y económica de utilizar o instalar recursos que compitan entre sí, a la vista del ritmo de desarrollo del mercado, teniendo en cuenta la naturaleza y el tipo de interconexión o acceso de que se trate, incluida la viabilidad de otros productos de acceso previo, como el acceso a conductos,

b) la posibilidad de proporcionar el acceso propuesto, en relación con la capacidad disponible,

c) la inversión inicial del propietario de los recursos, sin olvidar las inversiones públicas realizadas ni los riesgos inherentes a las inversiones,

d) la necesidad de salvaguardar la competencia a largo plazo, prestando especial atención a la competencia económicamente eficiente basada en las infraestructuras,

e) cuando proceda, los derechos pertinentes en materia de propiedad intelectual, y

f) el suministro de servicios paneuropeos.

4. Cuando la Comisión Nacional de los Mercados y la Competencia imponga obligaciones específicas a un operador de redes públicas de comunicaciones electrónicas para que facilite acceso podrá establecer determinadas condiciones técnicas u operativas al citado operador o a los beneficiarios de dicho acceso siempre que ello sea necesario para garantizar el funcionamiento normal de la red, conforme se establezca mediante real decreto. Las obligaciones de atenerse a normas o especificaciones técnicas concretas estarán de acuerdo con las normas a que se refiere el artículo 11.

5. Mediante real decreto, el Gobierno identificará las obligaciones específicas que la Comisión Nacional de los Mercados y la Competencia podrá imponer en los mercados de referencia considerados en este artículo y determinará las condiciones para su imposición, modificación o supresión.

Artículo 15. *Resolución de conflictos.*

1. La Comisión Nacional de los Mercados y la Competencia resolverá los conflictos que se susciten en relación con las obligaciones existentes en virtud de la presente Ley y su normativa de desarrollo entre operadores o entre operadores y otras entidades que se beneficien de las obligaciones de acceso e interconexión, de acuerdo con la definición que se da a los conceptos de acceso e interconexión en el anexo II de la presente Ley.

La Comisión Nacional de los Mercados y la Competencia, previa audiencia de las partes, dictará resolución vinculante sobre los extremos objeto del conflicto, en el plazo indicado en

la Ley de creación de esta Comisión, sin perjuicio de que puedan adoptarse medidas provisionales hasta el momento en que se dicte la resolución definitiva.

2. En caso de producirse un conflicto transfronterizo en el que una de las partes esté radicada en otro Estado miembro de la Unión Europea, la Comisión Nacional de los Mercados y la Competencia, en caso de que cualquiera de las partes así lo solicite, coordinará, en los términos que se establezcan mediante real decreto, sus esfuerzos para encontrar una solución al conflicto con la otra u otras autoridades nacionales de reglamentación afectadas.

La Comisión Nacional de los Mercados y la Competencia podrá solicitar que el ORECE adopte un dictamen sobre las medidas que deben tomarse para resolver el litigio.

Cuando se haya transmitido al ORECE tal solicitud, la Comisión Nacional de los Mercados y la Competencia deberá esperar el dictamen del ORECE antes de tomar medidas para resolver el litigio. Ello no constituirá un obstáculo para que la Comisión Nacional de los Mercados y la Competencia adopte medidas urgentes en caso necesario.

Cualquier obligación impuesta a una empresa por la Comisión Nacional de los Mercados y la Competencia en la resolución de un litigio deberá tener en cuenta en la mayor medida posible el dictamen adoptado por el ORECE.

CAPÍTULO IV

Separación funcional

Artículo 16. *Separación funcional obligatoria.*

1. Cuando la Comisión Nacional de los Mercados y la Competencia llegue a la conclusión de que las obligaciones específicas impuestas, en virtud de lo dispuesto en el artículo 14, no han bastado para conseguir una competencia efectiva y que sigue habiendo problemas de competencia importantes y persistentes o fallos del mercado en relación con mercados al por mayor de productos de acceso, podrá decidir la imposición, como medida excepcional, a los operadores con poder significativo en el mercado integrados verticalmente, de la obligación de traspasar las actividades relacionadas con el suministro al por mayor de productos de acceso a una unidad empresarial que actúe independientemente.

Esa unidad empresarial suministrará productos y servicios de acceso a todas las empresas, incluidas otras unidades empresariales de la sociedad matriz, en los mismos plazos, términos y condiciones, en particular en lo que se refiere a niveles de precios y de servicio, y mediante los mismos sistemas y procesos.

La imposición de la obligación de separación funcional prevista en el presente artículo se entenderá sin perjuicio de las medidas estructurales que se pudieran adoptar en aplicación de la normativa en materia de competencia.

2. Cuando la Comisión Nacional de los Mercados y la Competencia se proponga imponer una obligación de separación funcional, elaborará una propuesta que incluya:

a) motivos que justifiquen las conclusiones a las que ha llegado,

b) razones por las que hay pocas posibilidades, o ninguna, de competencia basada en la infraestructura en un plazo razonable,

c) un análisis del impacto previsto sobre la autoridad reguladora, sobre la empresa, particularmente en lo que se refiere a los trabajadores de la empresa separada y al sector de las comunicaciones electrónicas en su conjunto, sobre los incentivos para invertir en el sector en su conjunto, en especial por lo que respecta a la necesidad de garantizar la cohesión social y territorial, así como sobre otras partes interesadas, incluido en particular el impacto previsto sobre la competencia en infraestructuras y cualquier efecto negativo potencial sobre los consumidores, y

d) un análisis de las razones que justifiquen que esta obligación es el medio más adecuado para aplicar soluciones a los problemas de competencia o fallos del mercado que se hayan identificado.

3. El proyecto de medida incluirá los elementos siguientes:

a) la naturaleza y el grado precisos de la separación, especificando en particular el estatuto jurídico de la entidad empresarial separada,

b) una indicación de los activos de la entidad empresarial separada y de los productos o servicios que debe suministrar esta entidad,

c) los mecanismos de gobernanza para garantizar la independencia del personal empleado por la entidad empresarial separada y la estructura de incentivos correspondiente,

d) las normas para garantizar el cumplimiento de las obligaciones,

e) las normas para garantizar la transparencia de los procedimientos operativos, en particular de cara a otras partes interesadas, y

f) un programa de seguimiento para garantizar el cumplimiento, incluida la publicación de un informe anual.

4. La propuesta de imposición de la obligación de separación funcional, una vez que el Ministerio de Industria, Energía y Turismo y el Ministerio de Economía y Competitividad, como Autoridades Nacionales de Reglamentación identificadas en el apartado 1 del artículo 68, hayan emitido informe sobre la misma, se presentará a la Comisión Europea.

5. Tras la decisión de la Comisión Europea, la Comisión Nacional de los Mercados y la Competencia llevará a cabo, de conformidad con el procedimiento previsto en el artículo 13, un análisis coordinado de los distintos mercados relacionados con la red de acceso. Sobre la base de su evaluación, previo informe del Ministerio de Industria, Energía y Turismo y del Ministerio de Economía y Competitividad, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones específicas correspondientes.

Artículo 17. *Separación funcional voluntaria.*

1. En el supuesto de que una empresa designada como poseedora de poder significativo en uno o varios mercados pertinentes se proponga transferir sus activos de red de acceso local, o una parte sustancial de los mismos, a una persona jurídica separada de distinta propiedad, o establecer una entidad empresarial separada para suministrar a todos los proveedores minoristas, incluidas sus propias divisiones minoristas, productos de acceso completamente equivalentes, deberá informar con anterioridad al Ministerio de Industria, Energía y Turismo, al Ministerio de Economía y Competitividad y a la Comisión Nacional de los Mercados y la Competencia. Las empresas informarán también al Ministerio de Industria, Energía y Turismo, al Ministerio de Economía y Competitividad y a la Comisión Nacional de los Mercados y la Competencia de cualquier cambio de dicho propósito, así como del resultado final del proceso de separación.

2. En el caso de que se realice la separación funcional voluntaria, la Comisión Nacional de los Mercados y la Competencia evaluará el efecto de la transacción prevista sobre las obligaciones reglamentarias impuestas a esa entidad, llevando a cabo, de conformidad con el procedimiento previsto en el artículo 14, un análisis coordinado de los distintos mercados relacionados con la red de acceso. Sobre la base de su evaluación, previo informe del Ministerio de Industria, Energía y Turismo, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones específicas correspondientes.

Artículo 18. *Obligaciones específicas adicionales a la separación funcional.*

Las empresas a las que se haya impuesto o que hayan decidido la separación funcional podrán estar sujetas a cualquiera de las obligaciones específicas enumeradas en el artículo 14 en cualquier mercado de referencia en que hayan sido designadas como poseedoras de poder significativo en el mercado.

CAPÍTULO V

Numeración, direccionamiento y denominación

Artículo 19. *Principios generales.*

1. Para los servicios de comunicaciones electrónicas disponibles al público se proporcionarán los números, direcciones y nombres que se necesiten para permitir su

efectiva prestación, tomándose esta circunstancia en consideración en los planes nacionales correspondientes y en sus disposiciones de desarrollo.

2. Sin perjuicio de lo dispuesto en el apartado anterior, la regulación de los nombres de dominio de internet bajo el indicativo del país correspondiente a España («.es») se regirá por su normativa específica.

3. Corresponde al Gobierno la aprobación por real decreto de los planes nacionales de numeración, direccionamiento y denominación, teniendo en cuenta las decisiones aplicables que se adopten en el seno de las organizaciones y los foros internacionales.

4. Corresponde al Ministerio de Industria, Energía y Turismo la elaboración de las propuestas de planes nacionales para su elevación al Gobierno, y el desarrollo normativo de estos planes que podrán establecer condiciones asociadas a la utilización de los recursos públicos de numeración, direccionamiento y denominación, en particular la designación del servicio para el que se utilizarán estos recursos, incluyendo cualquier requisito relacionado con el suministro de dicho servicio.

5. Corresponde al Ministerio de Industria, Energía y Turismo el otorgamiento de los derechos de uso de los recursos públicos regulados en los planes nacionales de numeración, direccionamiento y denominación.

Los procedimientos para el otorgamiento de estos derechos serán abiertos, objetivos, no discriminatorios, proporcionados y transparentes. Estos procedimientos se establecerán mediante real decreto.

Las decisiones relativas a los otorgamientos de derechos de uso se adoptarán, comunicarán y harán públicas en el plazo máximo de tres semanas desde la recepción de la solicitud completa, salvo cuando se apliquen procedimientos de selección comparativa o competitiva, en cuyo caso, el plazo máximo será de seis semanas desde el fin del plazo de recepción de ofertas. Transcurrido el plazo máximo sin haberse notificado la resolución expresa, se podrá entender desestimada la solicitud por silencio administrativo. Asimismo, también se harán públicas las decisiones que se adopten relativas a la cancelación de derechos de uso.

6. Los operadores que presten servicios telefónicos disponibles al público u otros servicios que permitan efectuar y recibir llamadas a números del plan nacional de numeración telefónica deberán cursar las llamadas que se efectúen a los rangos de numeración telefónica nacional y, cuando permitan llamadas internacionales, al espacio europeo de numeración telefónica y a otros rangos de numeración internacional, en los términos que se especifiquen en los planes nacionales de numeración o en sus disposiciones de desarrollo, sin perjuicio del derecho del usuario de desconexión de determinados servicios.

Los operadores que presten servicios telefónicos disponibles al público u otros servicios que permitan las llamadas internacionales adoptarán las medidas oportunas para que sean cursadas cuantas llamadas se efectúen procedentes de y con destino al espacio europeo de numeración telefónica, a tarifas similares a las que se aplican a las llamadas con origen o destino en otros países comunitarios.

7. El otorgamiento de derechos de uso de los recursos públicos de numeración, direccionamiento y denominación regulados en los planes nacionales no supondrá el otorgamiento de más derechos que los de su utilización conforme a lo que se establece en esta Ley.

8. Los operadores a los que se haya otorgado el derecho de uso de una serie de números no podrán discriminar a otros operadores en lo que se refiere a las secuencias de números utilizadas para dar acceso a los servicios de éstos.

9. Todos los operadores y, en su caso, los fabricantes y los comerciantes estarán obligados a tomar las medidas necesarias para el cumplimiento de las decisiones que se adopten por el Ministerio de Industria, Energía y Turismo en materia de numeración, direccionamiento y denominación.

10. Los usuarios finales tendrán, en los términos que determine la normativa de desarrollo de la Ley, acceso a los recursos públicos regulados en los planes nacionales. Esta normativa podrá prever, cuando esté justificado, el otorgamiento de derechos de uso de números, nombres o direcciones a los usuarios finales para determinados rangos que a tal efecto se definan en los planes nacionales o en sus disposiciones de desarrollo.

11. Los operadores que exploten redes públicas de comunicaciones o presten servicios telefónicos disponibles al público, siempre que sea técnica y económicamente posible, adoptarán las medidas que sean necesarias para que los usuarios finales puedan tener acceso a los servicios utilizando números no geográficos en la Unión Europea, y que puedan tener acceso, con independencia de la tecnología y los dispositivos utilizados por el operador, a todos los números proporcionados en la Unión Europea, incluidos los de los planes nacionales de numeración de los Estados miembros, los del espacio europeo de numeración telefónica, y los Números Universales Internacionales de Llamada Gratuita.

12. El Gobierno apoyará la armonización de determinados números o series de números concretos dentro de la Unión Europea cuando ello promueva al mismo tiempo el funcionamiento del mercado interior y el desarrollo de servicios paneuropeos.

Artículo 20. *Planes nacionales.*

1. Los planes nacionales y sus disposiciones de desarrollo designarán los servicios para los que puedan utilizarse los números y, en su caso, direcciones y nombres correspondientes, incluido cualquier requisito relacionado con la prestación de tales servicios y las condiciones asociadas a su uso, que serán proporcionadas y no discriminatorias. Asimismo, los planes nacionales y sus disposiciones de desarrollo podrán incluir los principios de fijación de precios y los precios máximos que puedan aplicarse a los efectos de garantizar la protección de los consumidores.

2. El contenido de los citados planes y el de los actos derivados de su desarrollo y gestión serán públicos, salvo en lo relativo a materias que puedan afectar a la seguridad nacional.

3. A fin de cumplir con las obligaciones y recomendaciones internacionales o para garantizar la disponibilidad suficiente de números, direcciones y nombres, el Ministro de Industria, Energía y Turismo podrá, mediante orden que se publicará con la debida antelación a su entrada en vigor, y previo informe preceptivo de la Comisión Nacional de los Mercados y la Competencia, modificar la estructura y la organización de los planes nacionales o, en ausencia de éstos o de planes específicos para cada servicio, establecer medidas sobre la utilización de los recursos numéricos y alfanuméricos necesarios para la prestación de los servicios. Se habrán de tener en cuenta, a tales efectos, los intereses de los afectados y los gastos de adaptación que, de todo ello, se deriven para los operadores y para los usuarios.

4. Los planes nacionales o sus disposiciones de desarrollo podrán establecer procedimientos de selección competitiva o comparativa para el otorgamiento de derechos de uso de números y nombres con valor económico excepcional o que sean particularmente apropiados para la prestación de determinados servicios de interés general. Estos procedimientos respetarán los principios de publicidad, concurrencia y no discriminación para todas las partes interesadas.

Artículo 21. *Conservación de los números telefónicos por los abonados.*

1. Los operadores garantizarán, de conformidad con lo establecido en el artículo 47, que los abonados con números del plan nacional de numeración telefónica puedan conservar, previa solicitud, los números que les hayan sido asignados, con independencia del operador que preste el servicio. Mediante real decreto se fijarán los supuestos a los que sea de aplicación la conservación de números, así como los aspectos técnicos y administrativos necesarios para que ésta se lleve a cabo. En aplicación de este real decreto y su normativa de desarrollo, la Comisión Nacional de los Mercados y de la Competencia podrá fijar, mediante circular, características y condiciones para la conservación de los números.

2. Los costes derivados de la actualización de los elementos de la red y de los sistemas necesarios para hacer posible la conservación de los números deberán ser sufragados por cada operador sin que, por ello, tengan derecho a percibir indemnización alguna. Los demás costes que produzca la conservación de los números telefónicos se repartirán, a través del oportuno acuerdo, entre los operadores afectados por el cambio. A falta de acuerdo, resolverá la Comisión Nacional de los Mercados y de la Competencia. Los precios de interconexión para la aplicación de las facilidades de conservación de los números habrán de estar orientados en función de los costes y, en caso de imponerse cuotas directas a los

abonados, no deberán tener, en ningún caso, efectos disuasorios para el uso de dichas facilidades.

Artículo 22. *Números armonizados para los servicios armonizados europeos de valor social.*

1. El Ministerio de Industria, Energía y Turismo promoverá el conocimiento por la población de los números armonizados europeos que comienzan por las cifras 116 y fomentará la prestación en España de los servicios de valor social para los que están reservados tales números, poniéndolos a disposición de los interesados en su prestación.

2. El Ministerio de Industria, Energía y Turismo adoptará las iniciativas pertinentes para que los usuarios finales con discapacidad puedan tener el mejor acceso posible a los servicios prestados a través de los números armonizados europeos que comienzan por las cifras 116. En la atribución de tales números, dicho Ministerio establecerá las condiciones que faciliten el acceso a los servicios que se presten a través de ellos por los usuarios finales con discapacidad.

Entre las referidas condiciones podrán incluirse, en función del servicio en concreto de valor social que se trate, la de posibilitar la comunicación total a través de voz, texto y video para que las personas con discapacidad sensorial no se queden excluidas.

3. Las administraciones públicas competentes en la regulación o supervisión de cada uno de los servicios que se presten a través de los números armonizados europeos que comienzan por las cifras 116 velarán por que los ciudadanos reciban una información adecuada sobre la existencia y utilización de estos servicios de valor social.

TÍTULO III

Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas

CAPÍTULO I

Obligaciones de servicio público

Sección 1.ª Delimitación

Artículo 23. *Delimitación de las obligaciones de servicio público.*

1. Este capítulo tiene por objeto garantizar la existencia de servicios de comunicaciones electrónicas disponibles al público, de adecuada calidad en todo el territorio nacional a través de una competencia y una libertad de elección reales, y hacer frente a las circunstancias en que las necesidades de los usuarios finales no se vean atendidas de manera satisfactoria por el mercado.

2. Los operadores se sujetarán al régimen de obligaciones de servicio público y de carácter público, de acuerdo con lo establecido en este título. Cuando se impongan obligaciones de servicio público, conforme a lo dispuesto en este capítulo, se aplicará con carácter supletorio el régimen establecido para la concesión de servicio público determinado por el texto refundido de la Ley de Contratos del Sector Público, aprobado por el real decreto Legislativo 3/2011, de 14 de noviembre.

3. El cumplimiento de las obligaciones de servicio público en la explotación de redes públicas y en la prestación de servicios de comunicaciones electrónicas para los que aquéllas sean exigibles se efectuará con respeto a los principios de igualdad, transparencia, no discriminación, continuidad, adaptabilidad, disponibilidad y permanencia y conforme a los términos y condiciones que mediante real decreto se determinen.

4. Corresponde al Ministerio de Industria, Energía y Turismo el control y el ejercicio de las facultades de la Administración relativas a las obligaciones de servicio público y de carácter público a que se refiere este artículo.

5. Cuando el Ministerio de Industria, Energía y Turismo constate que cualquiera de los servicios a que se refiere este artículo se está prestando en competencia, en condiciones de precio, cobertura y calidad de servicio similares a aquellas en que los operadores designados deben prestarlas, podrá, previo informe de la Comisión Nacional de los Mercados y de la Competencia y audiencia a los interesados, determinar el cese de su prestación como obligación de servicio público y, en consecuencia, de la financiación prevista para tales obligaciones.

Artículo 24. *Categorías de obligaciones de servicio público.*

Los operadores están sometidos a las siguientes categorías de obligaciones de servicio público:

a) El servicio universal en los términos contenidos en la sección 2.ª de este capítulo.

b) Otras obligaciones de servicio público impuestas por razones de interés general, en la forma y con las condiciones establecidas en la sección 3.ª de este capítulo.

Sección 2.ª El servicio universal

Artículo 25. *Concepto y ámbito de aplicación.*

1. Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible.

Bajo el mencionado concepto de servicio universal se deberá garantizar, en los términos y condiciones que mediante real decreto se determinen por el Gobierno, que:

a) Todos los usuarios finales puedan obtener una conexión a la red pública de comunicaciones electrónicas desde una ubicación fija siempre que sus solicitudes se consideren razonables en los términos que mediante real decreto se determinen y que, incluirán, entre otros factores, el coste de su provisión. La conexión debe permitir realizar comunicaciones de voz, fax y datos, a velocidad suficiente para acceder de forma funcional a Internet. La conexión a la red pública de comunicaciones con capacidad de acceso funcional a Internet deberá permitir comunicaciones de datos en banda ancha a una velocidad en sentido descendente de 1 Mbit por segundo. El Gobierno podrá actualizar esta velocidad de acuerdo con la evolución social, económica y tecnológica, y las condiciones de competencia en el mercado, teniendo en cuenta los servicios utilizados por la mayoría de los usuarios.

b) Se satisfagan todas las solicitudes razonables de prestación de un servicio telefónico disponible al público a través de la conexión a que se refiere el párrafo anterior, de modo que se permita efectuar y recibir llamadas nacionales e internacionales.

c) Se ponga a disposición de los abonados al servicio telefónico disponible al público una guía general de números de abonados, ya sea impresa o electrónica, o ambas, que se actualice, como mínimo, una vez al año. Mediante real decreto se determinarán los colectivos de abonados que pueden solicitar que se le entregue la guía impresa. Asimismo, que se ponga a disposición de todos los usuarios finales de dicho servicio, incluidos los usuarios de teléfonos públicos de pago, al menos un servicio de información general sobre números de abonados. Todos los abonados al servicio telefónico disponible al público tendrán derecho a figurar en la mencionada guía general, sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad.

d) Exista una oferta suficiente de teléfonos públicos de pago u otros puntos de acceso público a la telefonía vocal en todo el territorio nacional, que satisfaga razonablemente las necesidades de los usuarios finales en lo relativo a la cobertura geográfica, al número de aparatos u otros puntos de acceso, y a la calidad de los servicios, garantice la accesibilidad de estos teléfonos por los usuarios con discapacidades y permita efectuar gratuitamente llamadas de emergencia desde los teléfonos públicos de pago sin tener que utilizar ninguna forma de pago utilizando el número único de llamadas de emergencia 112 y otros números de emergencia españoles.

e) Los usuarios finales con discapacidad tengan acceso a los servicios incluidos en los párrafos b), c) y d) de este apartado, a un nivel equivalente al que disfrutan otros usuarios finales.

f) Se ofrezcan a los consumidores que sean personas físicas, de acuerdo con condiciones transparentes, públicas y no discriminatorias, opciones o paquetes de tarifas que difieran de las aplicadas en condiciones normales de explotación comercial con objeto de garantizar, en particular, que las personas con necesidades sociales especiales puedan tener acceso a la red y a los servicios que componen el concepto de servicio universal. Con el mismo objeto podrán aplicarse, cuando proceda, limitaciones de precios, tarifas comunes, equiparación geográfica u otros regímenes similares a las prestaciones incluidas en este artículo.

El Ministerio de Industria, Energía y Turismo supervisará la evolución y el nivel de la tarificación al público de los conceptos que forman parte del servicio universal, bien sean prestados por el operador designado, o bien se encuentren disponibles en el mercado en caso de que no se hayan designado operadores en relación con estos servicios, en particular en relación con los niveles nacionales de precios al consumo y de rentas.

2. Mediante real decreto se podrán adoptar medidas a fin de garantizar que los usuarios finales con discapacidad también puedan beneficiarse de la capacidad de elección de operadores de que disfruta la mayoría de los usuarios finales. Asimismo, podrán establecerse sistemas de ayuda directa a los consumidores que sean personas físicas con rentas bajas o con necesidades sociales especiales.

3. Todas las obligaciones que se incluyen en el servicio universal estarán sujetas a los mecanismos de financiación que se establecen en el artículo 27.

4. El Gobierno, de conformidad con la normativa comunitaria, podrá revisar el alcance de las obligaciones de servicio universal.

Artículo 26. *Designación de los operadores encargados de la prestación del servicio universal.*

1. Cuando la prestación de cualquiera de los elementos integrantes del servicio universal no quede garantizada por el libre mercado, el Ministerio de Industria, Energía y Turismo designará uno o más operadores para que garanticen la prestación eficiente de dichos elementos del servicio universal, de manera que quede cubierta la totalidad del territorio nacional. A estos efectos podrán designarse operadores diferentes para la prestación de diversos elementos del servicio universal y abarcar distintas zonas del territorio nacional.

2. El sistema de designación de operadores encargados de garantizar la prestación de los servicios, prestaciones y ofertas del servicio universal se establecerá mediante real decreto, con sujeción a los principios de eficiencia, objetividad, transparencia y no discriminación sin excluir a priori la designación de ninguna empresa. En todo caso, contemplará un mecanismo de licitación pública para dichos servicios, prestaciones y ofertas. Estos procedimientos de designación garantizarán que la prestación del servicio universal se haga de manera rentable y se podrán utilizar como medio para determinar el coste neto derivado de las obligaciones asignadas, a los efectos de lo dispuesto en el artículo 27.1.

3. Cuando el operador designado para la prestación del servicio universal se proponga entregar una parte o la totalidad de sus activos de red de acceso local a una persona jurídica separada de distinta propiedad, informará con la debida antelación al Ministerio de Industria, Energía y Turismo a fin de evaluar las repercusiones de la operación prevista en el suministro de acceso desde una ubicación fija y la prestación de servicios telefónicos, de conformidad con el artículo 25. El Ministerio de Industria, Energía y Turismo, como consecuencia de la evaluación realizada, podrá imponer, modificar o suprimir obligaciones al operador designado.

4. El Ministerio de Industria, Energía y Turismo podrá establecer objetivos de rendimiento aplicables al operador u operadores designados para la prestación del servicio universal.

5. El Ministerio de Industria, Energía y Turismo notificará a la Comisión Europea las obligaciones de servicio universal impuestas al operador u operadores designados para el

cumplimiento de obligaciones de servicio universal, así como los cambios relacionados con dichas obligaciones o con el operador u operadores designados.

Artículo 27. *Coste y financiación del servicio universal.*

1. La Comisión Nacional de los Mercados y la Competencia determinará si la obligación de la prestación del servicio universal puede implicar una carga injustificada para los operadores obligados a su prestación.

En caso de que se considere que puede existir dicha carga injustificada, el coste neto de prestación del servicio universal será determinado periódicamente por la Comisión Nacional de los Mercados y la Competencia de acuerdo con los procedimientos de designación previstos en el artículo 26.2 o en función del ahorro neto que el operador conseguiría si no tuviera la obligación de prestar el servicio universal.

Para la determinación de este ahorro neto la Comisión Nacional de los Mercados y la Competencia desarrollará y publicará una metodología de acuerdo con los criterios que se establezcan mediante real decreto.

2. El coste neto de la obligación de prestación del servicio universal será financiado por un mecanismo de reparto, en condiciones de transparencia y no discriminación, por aquellos operadores que obtengan por la explotación de redes o la prestación de servicios de comunicaciones electrónicas unos ingresos brutos de explotación anuales superiores a 100 millones de euros. Esta cifra podrá ser actualizada o modificada mediante real decreto acordado en Consejo de Ministros, previo informe de la Comisión Nacional de los Mercados y la Competencia, en función de la evolución del mercado y de las cuotas que los distintos operadores tienen en cada momento en el mercado.

3. Una vez fijado este coste, la Comisión Nacional de los Mercados y la Competencia determinará las aportaciones que correspondan a cada uno de los operadores con obligaciones de contribución a la financiación del servicio universal.

Dichas aportaciones, así como, en su caso, las deducciones y exenciones aplicables, se verificarán de acuerdo con las condiciones que se establezcan por real decreto.

Las aportaciones recibidas se depositarán en el Fondo nacional del servicio universal, que se crea por esta Ley.

4. El Fondo nacional del servicio universal tiene por finalidad garantizar la financiación del servicio universal. Los activos en metálico procedentes de los operadores con obligaciones de contribuir a la financiación del servicio universal se depositarán en este fondo, en una cuenta específica designada a tal efecto. Los gastos de gestión de esta cuenta serán deducidos de su saldo, y los rendimientos que éste genere, si los hubiere, minorarán la contribución de los aportantes.

En la cuenta podrán depositarse aquellas aportaciones que sean realizadas por cualquier persona física o jurídica que desee contribuir, desinteresadamente, a la financiación de cualquier prestación propia del servicio universal.

Los operadores sujetos a obligaciones de prestación del servicio universal recibirán de este fondo la cantidad correspondiente al coste neto que les supone dicha obligación, calculado según el procedimiento establecido en este artículo.

La Comisión Nacional de los Mercados y la Competencia se encargará de la gestión del Fondo nacional del servicio universal. Mediante real decreto se determinará su estructura, organización, mecanismos de control y la forma y plazos en los que se realizarán las aportaciones.

5. Mediante real decreto podrá preverse la existencia de un mecanismo de compensación directa entre operadores para aquellos casos en que la magnitud del coste no justifique los costes de gestión del fondo nacional del servicio universal.

Sección 3.ª Otras obligaciones de servicio público

Artículo 28. *Otras obligaciones de servicio público.*

1. El Gobierno podrá, por necesidades de la defensa nacional, de la seguridad pública, seguridad vial o de los servicios que afecten a la seguridad de las personas o a la protección

civil, imponer otras obligaciones de servicio público distintas de las de servicio universal a los operadores.

2. El Gobierno podrá, asimismo, imponer otras obligaciones de servicio público, previo informe de la Comisión Nacional de los Mercados y la Competencia, así como de la administración territorial competente, motivadas por:

a) Razones de cohesión territorial.

b) Razones de extensión del uso de nuevos servicios y tecnologías, en especial a la sanidad, a la educación, a la acción social y a la cultura.

c) Por la necesidad de facilitar la comunicación entre determinados colectivos que se encuentren en circunstancias especiales y estén insuficientemente atendidos con la finalidad de garantizar la suficiencia de su oferta.

d) Por la necesidad de facilitar la disponibilidad de servicios que comporten la acreditación de fehaciencia del contenido del mensaje remitido o de su remisión o recepción.

3. Mediante real decreto se regulará el procedimiento de imposición de las obligaciones a las que se refiere el apartado anterior y su forma de financiación.

4. En cualquier caso, la obligación de encaminar las llamadas a los servicios de emergencia sin derecho a contraprestación económica de ningún tipo debe ser asumida tanto por los operadores que presten servicios de comunicaciones electrónicas al público para efectuar llamadas nacionales a números de un plan nacional de numeración telefónica, como por los que exploten redes públicas de comunicaciones electrónicas. Esta obligación se impone a dichos operadores respecto de las llamadas dirigidas al número telefónico 112 de atención a emergencias y a otros que se determinen mediante real decreto, incluidas aquellas que se efectúen desde teléfonos públicos de pago, sin que sea necesario utilizar ninguna forma de pago en estos casos.

En todo caso, el servicio de llamadas de emergencia será gratuito para los usuarios, cualquiera que sea la Administración pública responsable de su prestación y con independencia del tipo de terminal que se utilice.

Asimismo, los operadores pondrán gratuitamente a disposición de las autoridades receptoras de dichas llamadas la información que mediante real decreto se determine relativa a la ubicación de su procedencia.

Mediante real decreto se establecerán criterios para la precisión y la fiabilidad de la información facilitada sobre la ubicación de las personas que efectúan llamadas a los servicios de emergencia.

El acceso a los servicios de emergencia para los usuarios finales con discapacidad será equivalente al que disfrutan otros usuarios finales.

Las autoridades responsables de la prestación de los servicios 112 velarán por que los ciudadanos reciban una información adecuada sobre la existencia y utilización de este número, en particular, mediante iniciativas específicamente dirigidas a las personas que viajen a otros Estados miembros de la Unión Europea.

CAPÍTULO II

Derechos de los operadores y despliegue de redes públicas de comunicaciones electrónicas

Sección 1.ª Derechos de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y al establecimiento a su favor de servidumbres y de limitaciones a la propiedad

Artículo 29. *Derecho de ocupación de la propiedad privada.*

1. Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación de la propiedad privada cuando resulte estrictamente necesario para la instalación de la red en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas técnica o económicamente viables, ya sea a través de su expropiación forzosa o mediante la declaración de servidumbre forzosa de paso para la instalación de infraestructura de redes públicas de comunicaciones electrónicas. En ambos casos tendrán

la condición de beneficiarios en los expedientes que se tramiten, conforme a lo dispuesto en la legislación sobre expropiación forzosa.

Los operadores asumirán los costes a los que hubiera lugar por esta ocupación.

La ocupación de la propiedad privada se llevará a cabo tras la instrucción y resolución por el Ministerio de Industria, Energía y Turismo del oportuno procedimiento, en que deberán cumplirse todos los trámites y respetarse todas las garantías establecidas a favor de los titulares afectados en la legislación de expropiación forzosa.

2. La aprobación por el órgano competente del Ministerio de Industria, Energía y Turismo del proyecto técnico para la ocupación de propiedad privada llevará implícita, en cada caso concreto, la declaración de utilidad pública y la necesidad de ocupación para la instalación de redes públicas de comunicaciones electrónicas, a efectos de lo previsto en la legislación de expropiación forzosa.

3. Con carácter previo a la aprobación del proyecto técnico, se recabará informe del órgano de la comunidad autónoma competente en materia de ordenación del territorio, que habrá de ser emitido en el plazo máximo de 30 días hábiles desde su solicitud. Si el proyecto afecta a un área geográfica relevante o pudiera tener afecciones ambientales, este plazo será ampliado hasta tres meses. Asimismo, se recabará informe de los Ayuntamientos afectados sobre compatibilidad del proyecto técnico con la ordenación urbanística vigente, que deberá ser emitido en el plazo de 30 días desde la recepción de la solicitud.

4. En las expropiaciones que se lleven a cabo para la instalación de redes públicas de comunicaciones electrónicas ligadas de manera específica al cumplimiento de obligaciones de servicio público se seguirá el procedimiento especial de urgencia establecido en la Ley de Expropiación Forzosa, cuando así se haga constar en la resolución del órgano competente del Ministerio de Industria, Energía y Turismo que apruebe el oportuno proyecto técnico.

Artículo 30. *Derecho de ocupación del dominio público.*

Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación del dominio público en la medida en que ello sea necesario para el establecimiento de la red pública de comunicaciones electrónicas de que se trate.

Los titulares del dominio público garantizarán el acceso de todos los operadores a dicho dominio en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso u ocupación de dicho dominio público en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En particular, la ocupación o el derecho de uso de dominio público para la instalación o explotación de una red no podrá ser otorgado o asignado mediante procedimientos de licitación.

Artículo 31. *Normativa aplicable a la ocupación del dominio público y la propiedad privada.*

1. La normativa dictada por cualquier Administración Pública que afecte al despliegue de redes públicas de comunicaciones electrónicas deberá, en todo caso, reconocer el derecho de ocupación del dominio público o la propiedad privada para el despliegue de las redes públicas de comunicaciones electrónicas de conformidad con lo dispuesto en este título.

2. Las normas que se dicten por las correspondientes Administraciones, de conformidad con lo dispuesto en el apartado anterior, deberán cumplir, al menos, los siguientes requisitos:

a) Ser publicadas en un diario oficial del ámbito correspondiente a la Administración competente así como en la página web de dicha Administración Pública y, en todo caso, ser accesibles por medios electrónicos.

b) Prever un procedimiento rápido, sencillo, eficiente y no discriminatorio de resolución de las solicitudes de ocupación, que no podrá exceder de seis meses contados a partir de la presentación de la solicitud, salvo en caso de expropiación.

c) Garantizar la transparencia de los procedimientos y que las normas aplicables fomenten una competencia leal y efectiva entre los operadores.

d) Garantizar el respeto de los límites impuestos a la intervención administrativa en esta Ley en protección de los derechos de los operadores. En particular, la exigencia de documentación que los operadores deban aportar deberá ser motivada, tener una

justificación objetiva, ser proporcionada al fin perseguido y limitarse a lo estrictamente necesario.

3. Si las administraciones públicas reguladoras o titulares del dominio público a que se refiere este artículo ostentan la propiedad, total o parcial, o ejercen el control directo o indirecto de operadores que explotan redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, deberán mantener una separación estructural entre dichos operadores y los órganos encargados de la regulación y gestión de los derechos de utilización del dominio público correspondiente.

Artículo 32. *Ubicación compartida y uso compartido de la propiedad pública o privada.*

1. Los operadores de comunicaciones electrónicas podrán celebrar de manera voluntaria acuerdos entre sí para determinar las condiciones para la ubicación o el uso compartido de sus infraestructuras, con plena sujeción a la normativa de defensa de la competencia.

Las administraciones públicas fomentarán la celebración de acuerdos voluntarios entre operadores para la ubicación compartida y el uso compartido de infraestructuras situadas en bienes de titularidad pública o privada, en particular con vistas al despliegue de elementos de las redes rápidas y ultrarrápidas de comunicaciones electrónicas.

2. La ubicación compartida de infraestructuras y recursos asociados y la utilización compartida del dominio público o la propiedad privada también podrá ser impuesta de manera obligatoria a los operadores que tengan derecho a la ocupación de la propiedad pública o privada. A tal efecto, en los términos en que mediante real decreto se determine, el Ministerio de Industria, Energía y Turismo, previo trámite de audiencia a los operadores afectados y de manera motivada, podrá imponer, con carácter general o para casos concretos, la utilización compartida del dominio público o la propiedad privada en que se van a establecer las redes públicas de comunicaciones electrónicas o el uso compartido de las infraestructuras y recursos asociados.

Cuando una Administración pública competente considere que por razones de medio ambiente, salud pública, seguridad pública u ordenación urbana y territorial procede la imposición de la utilización compartida del dominio público o la propiedad privada, podrá instar de manera motivada al Ministerio de Industria, Energía y Turismo el inicio del procedimiento establecido en el párrafo anterior. En estos casos, antes de que el Ministerio de Industria, Energía y Turismo imponga la utilización compartida del dominio público o la propiedad privada, el citado departamento ministerial deberá realizar un trámite para que la Administración pública competente que ha instado el procedimiento pueda efectuar alegaciones por un plazo de 15 días hábiles.

3. Las medidas adoptadas de conformidad con el presente artículo deberán ser objetivas, transparentes, no discriminatorias y proporcionadas. Cuando proceda, estas medidas se aplicarán de forma coordinada con las Administraciones competentes correspondientes.

Artículo 33. *Otras servidumbres y limitaciones a la propiedad.*

1. La protección del dominio público radioeléctrico tiene como finalidades su aprovechamiento óptimo, evitar su degradación y el mantenimiento de un adecuado nivel de calidad en el funcionamiento de los distintos servicios de radiocomunicaciones.

Podrán establecerse las limitaciones a la propiedad y a la intensidad de campo eléctrico y las servidumbres que resulten necesarias para la protección radioeléctrica de determinadas instalaciones o para asegurar el adecuado funcionamiento de estaciones o instalaciones radioeléctricas utilizadas para la prestación de servicios públicos, por motivos de seguridad pública o cuando así sea necesario en virtud de acuerdos internacionales, en los términos de la disposición adicional segunda y las normas de desarrollo de esta Ley.

2. Asimismo podrán imponerse límites a los derechos de uso del dominio público radioeléctrico para la protección de otros bienes jurídicamente protegidos prevalentes o de servicios públicos que puedan verse afectados por la utilización de dicho dominio público, en los términos que mediante real decreto se determinen. En la imposición de estos límites se debe efectuar un previo trámite de audiencia a los titulares de los derechos de uso del

dominio público radioeléctrico que pueden verse afectados y se deberán respetar los principios de transparencia y publicidad.

Sección 2.ª Normativa de las administraciones públicas que afecte al despliegue de redes públicas de comunicaciones electrónicas

Artículo 34. *Colaboración entre administraciones públicas en el despliegue de las redes públicas de comunicaciones electrónicas.*

1. La Administración del Estado y las administraciones públicas deberán colaborar a través de los mecanismos previstos en la presente Ley y en el resto del ordenamiento jurídico, a fin de hacer efectivo el derecho de los operadores de comunicaciones electrónicas de ocupar la propiedad pública y privada para realizar el despliegue de redes públicas de comunicaciones electrónicas.

2. Las redes públicas de comunicaciones electrónicas constituyen equipamiento de carácter básico y su previsión en los instrumentos de planificación urbanística tiene el carácter de determinaciones estructurantes. Su instalación y despliegue constituyen obras de interés general.

3. La normativa elaborada por las administraciones públicas que afecte al despliegue de las redes públicas de comunicaciones electrónicas y los instrumentos de planificación territorial o urbanística deberán recoger las disposiciones necesarias para impulsar o facilitar el despliegue de infraestructuras de redes de comunicaciones electrónicas en su ámbito territorial, en particular, para garantizar la libre competencia en la instalación de redes y en la prestación de servicios de comunicaciones electrónicas y la disponibilidad de una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras.

De esta manera, dicha normativa o instrumentos de planificación no podrán establecer restricciones absolutas o desproporcionadas al derecho de ocupación del dominio público y privado de los operadores ni imponer soluciones tecnológicas concretas, itinerarios o ubicaciones concretas en los que instalar infraestructuras de red de comunicaciones electrónicas. En este sentido, cuando una condición pudiera implicar la imposibilidad de llevar a cabo la ocupación del dominio público o la propiedad privada, el establecimiento de dicha condición deberá estar plenamente justificado e ir acompañado de las alternativas necesarias para garantizar el derecho de ocupación de los operadores y su ejercicio en igualdad de condiciones.

Las administraciones públicas contribuirán a garantizar y hacer real una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras identificando dichos lugares y espacios físicos en los que poder cumplir el doble objetivo de que los operadores puedan ubicar sus infraestructuras de redes de comunicaciones electrónicas así como la obtención de un despliegue de las redes ordenado desde el punto de vista territorial.

4. La normativa elaborada por las administraciones públicas en el ejercicio de sus competencias que afecte al despliegue de las redes públicas de comunicaciones electrónicas y los instrumentos de planificación territorial o urbanística deberán cumplir con lo dispuesto en la normativa sectorial de telecomunicaciones. En particular, deberán respetar los parámetros y requerimientos técnicos esenciales necesarios para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas, establecidos en la disposición adicional undécima y en las normas reglamentarias aprobadas en materia de telecomunicaciones, y los límites en los niveles de emisión radioeléctrica tolerable fijados por el Estado.

En el ejercicio de su iniciativa normativa, cuando esta afecte al despliegue de redes públicas de comunicaciones electrónicas, las administraciones públicas actuarán de acuerdo con los principios de necesidad, proporcionalidad, seguridad jurídica, transparencia, accesibilidad, simplicidad y eficacia.

Los operadores no tendrán obligación de aportar la documentación o información de cualquier naturaleza que ya obre en poder de la Administración. El Ministerio de Industria, Energía y Turismo establecerá, mediante real decreto, la forma en que se facilitará a las

administraciones públicas la información que precisen para el ejercicio de sus propias competencias.

5. Los operadores deberán hacer uso de las canalizaciones subterráneas o en el interior de las edificaciones que permitan el despliegue y explotación de redes públicas de comunicaciones electrónicas.

En los casos en los que no existan dichas canalizaciones o no sea posible su uso por razones técnicas o económicas, los operadores podrán efectuar despliegues aéreos siguiendo los previamente existentes.

Igualmente, en los mismos casos, los operadores podrán efectuar por fachadas despliegue de cables y equipos que constituyan redes públicas de comunicaciones electrónicas y sus recursos asociados, si bien para ello deberán utilizar, en la medida de lo posible, los despliegues, canalizaciones, instalaciones y equipos previamente instalados.

Los despliegues aéreos y por fachadas no podrán realizarse en casos justificados de edificaciones del patrimonio histórico-artístico o que puedan afectar a la seguridad pública.

6. Para la instalación de las estaciones o infraestructuras radioeléctricas utilizadas para la prestación de servicios de comunicaciones electrónicas disponibles para el público a las que se refiere la disposición adicional tercera de la Ley 12/2012, de 26 de diciembre, de medidas urgentes de liberalización del comercio y de determinados servicios, no podrá exigirse la obtención de licencia previa de instalaciones, de funcionamiento o de actividad, ni otras de clase similar o análogas, en los términos indicados en la citada ley.

Para la instalación de redes públicas de comunicaciones electrónicas o de estaciones radioeléctricas en dominio privado distintas de las señaladas en el párrafo anterior, no podrá exigirse por parte de las administraciones públicas competentes la obtención de licencia o autorización previa de instalaciones, de funcionamiento o de actividad, o de carácter medioambiental, ni otras licencias o aprobaciones de clase similar o análogas que sujeten a previa autorización dicha instalación, en el caso de que el operador haya presentado a la administración pública competente para el otorgamiento de la licencia o autorización un plan de despliegue o instalación de red de comunicaciones electrónicas, en el que se contemplen dichas infraestructuras o estaciones, y siempre que el citado plan haya sido aprobado por dicha administración.

En el Plan de despliegue o instalación, el operador deberá prever los supuestos en los que se van a efectuar despliegues aéreos o por fachadas de cables y equipos en los términos indicados en el apartado anterior.

Este plan de despliegue o instalación a presentar por el operador se sujetará al contenido y deberá respetar las condiciones técnicas exigidas mediante real decreto acordado en Consejo de Ministros.

El plan de despliegue o instalación de red pública de comunicaciones electrónicas se entenderá aprobado si, **transcurridos dos meses desde su presentación**, la administración pública competente no ha dictado resolución expresa.

Las licencias o autorizaciones previas que, de acuerdo con los párrafos anteriores, no puedan ser exigidas, serán sustituidas por declaraciones responsables, de conformidad con lo establecido en el artículo 71 bis de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común, relativas al cumplimiento de las previsiones legales establecidas en la normativa vigente. En todo caso, el declarante deberá estar en posesión del justificante de pago del tributo correspondiente cuando sea preceptivo.

La declaración responsable deberá contener una manifestación explícita del cumplimiento de aquellos requisitos que resulten exigibles de acuerdo con la normativa vigente, incluido, en su caso, estar en posesión de la documentación que así lo acredite.

Cuando deban realizarse diversas actuaciones relacionadas con la infraestructura o estación radioeléctrica, las declaraciones responsables se tramitarán conjuntamente siempre que ello resulte posible.

La presentación de la declaración responsable, con el consiguiente efecto de habilitación a partir de ese momento para ejecutar la instalación, no prejuzgará en modo alguno la situación y efectivo acomodo de las condiciones de la infraestructura o estación radioeléctrica a la normativa aplicable, ni limitará el ejercicio de las potestades administrativas de comprobación, inspección, sanción, y, en general, de control que a la

administración en cualquier orden, estatal, autonómico o local, le estén atribuidas por el ordenamiento sectorial aplicable en cada caso.

La inexactitud, falsedad u omisión, de carácter esencial, en cualquier dato, manifestación o documento que se acompañe o incorpore a una declaración responsable, o la no presentación de la declaración responsable determinará la imposibilidad de explotar la instalación y, en su caso, la obligación de retirarla desde el momento en que se tenga constancia de tales hechos, sin perjuicio de las responsabilidades penales, civiles o administrativas a que hubiera lugar.

Reglamentariamente se establecerán los elementos de la declaración responsable que tendrán dicho carácter esencial.

Téngase en cuenta que se declara inconstitucional y nulo el inciso destacado del párrafo quinto del apartado 6 por Sentencia del TC 20/2016, de 4 de febrero. Ref. BOE-A-2016-2337.

7. En el caso de que sobre una infraestructura de red pública de comunicaciones electrónicas, fija o móvil, incluidas las estaciones radioeléctricas de comunicaciones electrónicas, ya esté ubicada en dominio público o privado, se realicen actuaciones de innovación tecnológica o adaptación técnica que supongan la incorporación de nuevo equipamiento o la realización de emisiones radioeléctricas en nuevas bandas de frecuencias o con otras tecnologías, sin variar los elementos de obra civil y mástil, no se requerirá ningún tipo de concesión, autorización o licencia nueva o modificación de la existente o declaración responsable o comunicación previa a las administraciones públicas competentes por razones de ordenación del territorio, urbanismo o medioambientales.

8. Cuando las administraciones públicas elaboren proyectos que impliquen la variación en la ubicación de una infraestructura o un elemento de la red de transmisión de comunicaciones electrónicas, deberán dar audiencia previa al operador titular de la infraestructura afectada, a fin de que realice las alegaciones pertinentes sobre los aspectos técnicos, económicos y de cualquier otra índole respecto a la variación proyectada.

Artículo 35. *Mecanismos de colaboración entre el Ministerio de Industria, Energía y Turismo y las administraciones públicas para el despliegue de las redes públicas de comunicaciones electrónicas.*

1. El Ministerio de Industria, Energía y Turismo y las administraciones públicas tienen los deberes de recíproca información y de colaboración y cooperación mutuas en el ejercicio de sus actuaciones de regulación y que puedan afectar a las telecomunicaciones, según lo establecido por el ordenamiento vigente.

Esta colaboración se articulará, entre otros, a través de los mecanismos establecidos en los siguientes apartados, que podrán ser complementados mediante acuerdos de coordinación y cooperación entre el Ministerio de Industria, Energía y Turismo y las administraciones públicas competentes, garantizando en todo caso un trámite de audiencia para los interesados.

2. Los órganos encargados de los procedimientos de aprobación, modificación o revisión de los instrumentos de planificación territorial o urbanística que afecten al despliegue de las redes públicas de comunicaciones electrónicas deberán recabar el oportuno informe del Ministerio de Industria, Energía y Turismo. Dicho informe versará sobre la adecuación de dichos instrumentos de planificación con la presente Ley y con la normativa sectorial de telecomunicaciones y sobre las necesidades de redes públicas de comunicaciones electrónicas en el ámbito territorial a que se refieran.

El referido informe preceptivo será previo a la aprobación del instrumento de planificación de que se trate y tendrá carácter vinculante en lo que se refiere a su adecuación a la normativa sectorial de telecomunicaciones, en particular, al régimen jurídico de las telecomunicaciones establecido por la presente Ley y su normativa de desarrollo, y a las necesidades de redes públicas de comunicaciones electrónicas, debiendo señalar expresamente los puntos y aspectos respecto de los cuales se emite con ese carácter vinculante.

El Ministerio de Industria, Energía y Turismo emitirá el informe en un plazo máximo de tres meses. Sin perjuicio de lo dispuesto en el artículo 83.4 de la Ley 30/1992, de 26 de noviembre, transcurrido dicho plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación del instrumento de planificación.

A falta de solicitud del preceptivo informe, no podrá aprobarse el correspondiente instrumento de planificación territorial o urbanística en lo que se refiere al ejercicio de las competencias estatales en materia de telecomunicaciones.

En el caso de que el informe no sea favorable, los órganos encargados de la tramitación de los procedimientos de aprobación, modificación o revisión de los instrumentos de planificación territorial o urbanística dispondrán de un plazo máximo de un mes, a contar desde la recepción del informe, para remitir al Ministerio de Industria, Energía y Turismo sus alegaciones al informe, motivadas por razones de medio ambiente, salud pública, seguridad pública u ordenación urbana y territorial.

El Ministerio de Industria, Energía y Turismo, a la vista de las alegaciones presentadas, emitirá un nuevo informe en el plazo máximo de un mes a contar desde la recepción de las alegaciones. Sin perjuicio de lo dispuesto en el artículo 83.4 de la Ley 30/1992, de 26 de noviembre, transcurrido dicho plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación del instrumento de planificación. El informe tiene carácter vinculante, de forma que si el informe vuelve a ser no favorable, no podrá aprobarse el correspondiente instrumento de planificación territorial o urbanística en lo que se refiere al ejercicio de las competencias estatales en materia de telecomunicaciones.

3. Mediante orden, el Ministro de Industria, Energía y Turismo podrá establecer la forma en que han de solicitarse los informes a que se refiere el apartado anterior y la información a facilitar por parte del órgano solicitante, en función del tipo de instrumento de planificación territorial o urbanística, pudiendo exigirse a las administraciones públicas competentes su tramitación por vía electrónica.

4. En la medida en que la instalación y despliegue de las redes de comunicaciones electrónicas constituyen obras de interés general, el conjunto de administraciones públicas tienen la obligación de facilitar el despliegue de infraestructuras de redes de comunicaciones electrónicas en su ámbito territorial, para lo cual deben dar debido cumplimiento a los deberes de recíproca información y de colaboración y cooperación mutuas en el ejercicio de sus actuaciones y de sus competencias.

En defecto de acuerdo entre las administraciones públicas, cuando quede plenamente justificada la necesidad de redes públicas de comunicaciones electrónicas, y siempre y cuando se cumplan los parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las redes y servicios de comunicaciones electrónicas establecidos en el apartado 4 del artículo anterior, el Consejo de Ministros podrá autorizar la ubicación o el itinerario concreto de una infraestructura de red de comunicaciones electrónicas, en cuyo caso la administración pública competente deberá incorporar necesariamente en sus respectivos instrumentos de ordenación las rectificaciones imprescindibles para acomodar sus determinaciones a aquéllas.

5. La tramitación por la administración pública competente de una medida cautelar que impida o paralice o de una resolución que deniegue la instalación de la infraestructura de red que cumpla los parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas establecidos en el apartado 4 del artículo anterior, excepto en edificaciones del patrimonio histórico-artístico, será objeto de previo informe preceptivo del Ministerio de Industria, Energía y Turismo, que dispone del plazo máximo de un mes para su emisión y que será evacuado tras, en su caso, los intentos que procedan de encontrar una solución negociada con los órganos encargados de la tramitación de la citada medida o resolución.

Sin perjuicio de lo dispuesto en el artículo 83.4 de la Ley 30/1992, de 26 de noviembre, transcurrido dicho plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación de la medida o resolución.

A falta de solicitud del preceptivo informe, así como en el supuesto de que el informe no sea favorable, no se podrá aprobar la medida o resolución.

6. El Ministerio de Industria, Energía y Turismo promoverá con la asociación de entidades locales de ámbito estatal con mayor implantación la elaboración de un modelo tipo de declaración responsable a que se refiere el apartado 6 del artículo anterior.

7. Igualmente, el Ministerio de Industria, Energía y Turismo aprobará recomendaciones para la elaboración por parte de las administraciones públicas competentes de las normas o instrumentos contemplados en la presente sección, que podrán contener modelos de ordenanzas municipales elaborados conjuntamente con la asociación de entidades locales de ámbito estatal con mayor implantación. En el caso de municipios se podrá reemplazar la solicitud de informe a que se refiere el apartado 2 de este artículo por la presentación al Ministerio de Industria, Energía y Turismo del proyecto de instrumento acompañado de la declaración del Alcalde del municipio acreditando el cumplimiento de dichas recomendaciones.

8. El Ministerio de Industria, Energía y Turismo podrá crear, mediante real decreto, un punto de información único a través del cual los operadores de comunicaciones electrónicas accederán por vía electrónica a toda la información relativa sobre las condiciones y procedimientos aplicables para la instalación y despliegue de redes de comunicaciones electrónicas y sus recursos asociados.

Las Comunidades Autónomas y las Corporaciones Locales podrán, mediante la suscripción del oportuno convenio de colaboración con el Ministerio de Industria, Energía y Turismo, adherirse al punto de información único, en cuyo caso, los operadores de comunicaciones electrónicas deberán presentar en formato electrónico a través de dicho punto las declaraciones responsables a que se refiere el apartado 6 del artículo anterior y permisos de toda índole para ocupar dominio público y privado necesario para el despliegue de dichas redes que vayan dirigidas a la respectiva Comunidad Autónoma o Corporación Local.

El punto de información único será gestionado por el Ministerio de Industria, Energía y Turismo y será el encargado de remitir a la Comunidad Autónoma o Corporación Local que se haya adherido a dicho punto todas las declaraciones responsables y solicitudes que para la instalación y despliegue de redes de comunicaciones electrónicas y sus recursos asociados les hayan presentado los operadores de comunicaciones electrónicas.

El Ministerio de Industria, Energía y Turismo, las Comunidades Autónomas y la asociación de entidades locales de ámbito estatal con mayor implantación fomentarán el uso de este punto de información único por el conjunto de las administraciones públicas con vistas a reducir cargas y costes administrativos, facilitar la interlocución de los operadores con la administración y simplificar el cumplimiento de los trámites administrativos.

Artículo 36. *Previsión de infraestructuras de comunicaciones electrónicas en proyectos de urbanización y en obras civiles financiadas con recursos públicos.*

1. Cuando se acometan proyectos de urbanización, el proyecto técnico de urbanización deberá prever la instalación de infraestructura de obra civil para facilitar el despliegue de las redes públicas de comunicaciones electrónicas, pudiendo incluir adicionalmente elementos y equipos de red pasivos en los términos que determine la normativa técnica de telecomunicaciones que se dicte en desarrollo de este artículo.

Las infraestructuras que se instalen para facilitar el despliegue de las redes públicas de comunicaciones electrónicas conforme al párrafo anterior formarán parte del conjunto resultante de las obras de urbanización y pasarán a integrarse en el dominio público municipal. La administración pública titular de dicho dominio público pondrá tales infraestructuras a disposición de los operadores interesados en condiciones de igualdad, transparencia y no discriminación.

Mediante real decreto se establecerá el dimensionamiento y características técnicas mínimas que habrán de reunir estas infraestructuras.

2. En las obras civiles financiadas total o parcialmente con recursos públicos se preverá, en los supuestos y condiciones que se determinen mediante real decreto, la instalación de recursos asociados y otras infraestructuras de obra civil para facilitar el despliegue de las redes públicas de comunicaciones electrónicas, que se pondrán a disposición de los operadores interesados en condiciones de igualdad, transparencia y no discriminación.

Sección 3.ª Acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas

Artículo 37. *Acceso a las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas.*

1. Las administraciones públicas titulares de infraestructuras susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas facilitarán el acceso a dichas infraestructuras, siempre que dicho acceso no comprometa la continuidad y seguridad de la prestación de los servicios de carácter público que en dichas infraestructuras realiza su titular, en condiciones objetivas, de transparencia y no discriminación a los operadores que instalen o exploten redes públicas de comunicaciones electrónicas, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso a las infraestructuras citadas en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En particular, el acceso a dichas infraestructuras para la instalación o explotación de una red no podrá ser otorgado o reconocido mediante procedimientos de licitación.

2. Las entidades o sociedades encargadas de la gestión de infraestructuras de transporte de competencia estatal, así como las empresas y operadores de otros sectores distintos al de las comunicaciones electrónicas que sean titulares o gestoras de infraestructuras en el dominio público del Estado, de las Comunidades Autónomas o de las Entidades Locales o beneficiarias de expropiaciones forzosas y que sean susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas facilitarán el acceso a dichas infraestructuras a los operadores que instalen o exploten redes públicas de comunicaciones electrónicas, siempre que dicho acceso no comprometa la continuidad y seguridad de la prestación de los servicios que en dichas infraestructuras realiza su titular. En particular, este acceso se reconoce en relación con las infraestructuras viarias, ferroviarias, puertos, aeropuertos, abastecimiento de agua, saneamiento, y del transporte y la distribución de gas y electricidad. El acceso deberá facilitarse en condiciones de igualdad, transparencia y no discriminación.

3. Por infraestructuras susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas se entenderán tubos, postes, conductos, cajas, cámaras, armarios, y cualquier recurso asociado que pueda ser utilizado para desplegar y albergar cables de comunicaciones electrónicas, equipos, dispositivos, o cualquier otro recurso análogo necesario para el despliegue e instalación de las redes.

4. Mediante real decreto se determinarán los procedimientos, plazos, requisitos y condiciones en los que se facilitará el acceso a las infraestructuras susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas, así como las causas por las que se pueda denegar dicho acceso.

5. El Ministerio de Industria, Energía y Turismo podrá exigir a las administraciones públicas y sus entidades y sociedades, así como a las empresas y operadores a que se refieren los dos primeros apartados de este artículo, que suministren la información necesaria para elaborar de forma coordinada un inventario detallado de la naturaleza, la disponibilidad y el emplazamiento geográfico de las infraestructuras susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas. Dicho inventario se facilitará a los operadores de redes y servicios de comunicaciones electrónicas.

6. Las partes negociarán libremente los acuerdos del acceso a que se refiere este artículo y sus condiciones, incluidas las contraprestaciones económicas. Cualquiera de las partes podrá presentar un conflicto sobre el acceso y sus condiciones ante la Comisión Nacional de los Mercados y la Competencia, la cual, previa audiencia de las partes, dictará resolución vinculante sobre los extremos objeto del conflicto, en el plazo indicado en la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, sin perjuicio de que puedan adoptarse medidas provisionales hasta el momento en que se dicte la resolución definitiva.

7. Las administraciones públicas titulares de las infraestructuras a las que se hace referencia en este artículo tendrán derecho a establecer las compensaciones económicas que correspondan por el uso que de ellas se haga por parte de los operadores.

Artículo 38. *Acceso o uso de las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal.*

1. Los órganos o entes pertenecientes a la Administración General del Estado así como cualesquiera otras entidades o sociedades encargados de la gestión de infraestructuras de transporte de competencia estatal que presten, directamente o a través de entidades o sociedades intermedias, servicios de comunicaciones electrónicas o comercialicen la explotación de redes públicas de comunicaciones electrónicas, negociarán con los operadores de redes y servicios de comunicaciones electrónicas interesados en el acceso o uso de las redes de comunicaciones electrónicas de las que aquellos sean titulares.

2. Las condiciones para el acceso o uso de estas redes han de ser equitativas, no discriminatorias, objetivas, transparentes, neutrales y a precios de mercado, siempre que se garantice al menos la recuperación de coste de las inversiones y su operación y mantenimiento, para todos los operadores de redes y servicios de comunicaciones electrónicas, incluidos los pertenecientes o vinculados a dichos órganos o entes, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso o uso a dichas redes en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En todo caso, deberá preservarse la seguridad de las infraestructuras de transporte en las que están instaladas las redes de comunicaciones electrónicas a que se refiere este artículo y de los servicios que en dichas infraestructuras se prestan.

3. Las partes acordarán libremente los acuerdos del acceso o uso a que se refiere este artículo, a partir de las condiciones establecidas en el apartado anterior. Cualquiera de las partes podrá presentar un conflicto sobre el acceso y sus condiciones ante la Comisión Nacional de los Mercados y la Competencia, la cual, previa audiencia de las partes, dictará resolución vinculante sobre los extremos objeto del conflicto, en el plazo indicado en la Ley de creación de dicha Comisión, sin perjuicio de que puedan adoptarse medidas provisionales hasta el momento en que se dicte la resolución definitiva.

CAPÍTULO III

Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

Artículo 39. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los

servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal.

9. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

10. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Industria, Energía y Turismo.

11. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

Artículo 40. *Interceptación de las comunicaciones electrónicas por los servicios técnicos.*

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico o para la localización de interferencias perjudiciales sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.

b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan deberán ser custodiados hasta la finalización, en su caso, del expediente sancionador que hubiera lugar o, en otro caso, destruidos inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 60.

Artículo 41. *Protección de los datos de carácter personal.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.

b) La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.

c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y

podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del proveedor de informar a los abonados o particulares afectados, si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación.

En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales.

Los operadores deberán llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado. Mediante real decreto podrá establecerse el formato y contenido del inventario.

A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar instrucciones sobre las circunstancias en que se requiere que el proveedor notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

Artículo 42. *Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 43. *Cifrado en las redes y servicios de comunicaciones electrónicas.*

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

Artículo 44. *Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.*

1. Los operadores de redes y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas.

2. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes.

3. Los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Industria, Energía y Turismo las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios.

Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a las empresas que lo hagan, en caso de estimar que la divulgación de la violación reviste interés público. Una vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado.

Del mismo modo, el Ministerio comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas. También el Ministerio comunicará a la Comisión Nacional de los Mercados y la Competencia las violaciones de la seguridad o pérdidas de integridad a que se refiere este apartado que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia.

4. El Ministerio de Industria, Energía y Turismo establecerá los mecanismos para supervisar el cumplimiento de las obligaciones anteriores y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para los operadores, incluidas las relativas a las fechas límite de aplicación, para que adopten determinadas medidas relativas a la integridad y seguridad de redes y servicios de comunicaciones electrónicas. Entre ellas, podrá imponer:

a) La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad.

b) La obligación de someterse a una auditoría de seguridad realizada por un organismo independiente o por una autoridad competente, y de poner el resultado a disposición del Ministerio de Industria, Energía y Turismo. El coste de la auditoría será sufragado por el operador.

5. En particular, los operadores garantizarán la mayor disponibilidad posible de los servicios telefónicos disponibles al público a través de las redes públicas de comunicaciones en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán todas las

medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia.

6. El presente artículo se entiende sin perjuicio de lo establecido en el apartado 4 del artículo 4 de la presente Ley.

CAPÍTULO IV

Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios

Artículo 45. *Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios.*

1. Mediante real decreto se desarrollará la normativa legal en materia de infraestructuras comunes de comunicaciones electrónicas en el interior de edificios y conjuntos inmobiliarios. Dicho real decreto determinará, tanto el punto de interconexión de la red interior con las redes públicas, como las condiciones aplicables a la propia red interior. Asimismo regulará las garantías aplicables al acceso a los servicios de comunicaciones electrónicas a través de sistemas individuales en defecto de infraestructuras comunes de comunicaciones electrónicas, y el régimen de instalación de éstas en todos aquellos aspectos no previstos en las disposiciones con rango legal reguladoras de la materia.

2. La normativa técnica básica de edificación que regule la infraestructura de obra civil en el interior de los edificios y conjuntos inmobiliarios deberá tomar en consideración las necesidades de soporte de los sistemas y redes de comunicaciones electrónicas fijadas de conformidad con la normativa a que se refiere el apartado 1, previendo que la infraestructura de obra civil disponga de capacidad suficiente para permitir el paso de las redes de los distintos operadores, de forma que se facilite la posibilidad de uso compartido de estas infraestructuras por aquéllos.

3. La normativa reguladora de las infraestructuras comunes de comunicaciones electrónicas promoverá la sostenibilidad de las edificaciones y conjuntos inmobiliarios, de uso residencial, industrial, terciario y dotacional, facilitando la introducción de aquellas tecnologías de la información y las comunicaciones que favorezcan su eficiencia energética, accesibilidad y seguridad, tendiendo hacia la implantación progresiva en España del concepto de hogar digital.

4. Los operadores podrán instalar los tramos finales de las redes fijas de comunicaciones electrónicas de acceso ultrarrápido así como sus recursos asociados en los edificios, fincas y conjuntos inmobiliarios que estén acogidos, o deban acogerse, al régimen de propiedad horizontal o a los edificios que, en todo o en parte, hayan sido o sean objeto de arrendamiento por plazo superior a un año, salvo los que alberguen una sola vivienda, al objeto de que cualquier copropietario o, en su caso, arrendatario del inmueble pueda hacer uso de dichas redes.

En el caso de edificios en los que no exista una infraestructura común de comunicaciones electrónicas en el interior del edificio o conjunto inmobiliario, o la existente no permita instalar el correspondiente acceso ultrarrápido, dicha instalación podrá realizarse haciendo uso de los elementos comunes de la edificación. En los casos en los que no sea posible realizar la instalación en el interior de la edificación o finca por razones técnicas o económicas, la instalación podrá realizarse utilizando las fachadas de las edificaciones.

El operador que se proponga instalar los tramos finales de red y sus recursos asociados a que se refiere el presente apartado, deberá comunicarlo por escrito a la comunidad de propietarios o, en su caso, al propietario del edificio, junto con un proyecto de la actuación que pretende realizar, antes de iniciar cualquier instalación. El formato, contenido, y plazos formales de presentación tanto de la comunicación escrita como del proyecto de actuación referidos en el presente párrafo serán determinados reglamentariamente. En todo caso, corresponderá al operador acreditar que la comunicación escrita ha sido entregada.

La instalación no podrá realizarse si en el plazo de un mes desde que la comunicación se produzca, la comunidad de propietarios o el propietario acredita ante el operador que ninguno de los copropietarios o arrendatarios del edificio está interesado en disponer de las infraestructuras propuestas, o afirma que va a realizar, dentro de los tres meses siguientes a

la contestación, la instalación de una infraestructura común de comunicaciones electrónicas en el interior del edificio o la adaptación de la previamente existente que permitan dicho acceso ultrarrápido. Transcurrido el plazo de un mes antes señalado desde que la comunicación se produzca sin que el operador hubiera obtenido respuesta, o el plazo de tres meses siguientes a la contestación sin que se haya realizado la instalación de la infraestructura común de comunicaciones electrónicas, el operador estará habilitado para iniciar la instalación de los tramos finales de red y sus recursos asociados, si bien será necesario que el operador indique a la comunidad de propietarios o al propietario el día de inicio de la instalación.

El procedimiento del párrafo anterior no será aplicable al operador que se proponga instalar los tramos finales de red fija de comunicaciones electrónicas de acceso ultrarrápido y sus recursos asociados en un edificio o conjunto inmobiliario en el que otro operador haya iniciado o instalado tramos finales de dichas redes; o en aquellos casos en los que se trate de un tramo para dar continuidad a una instalación que sea necesaria para proporcionar acceso a dichas redes en edificios o fincas colindantes o cercanas y no exista otra alternativa económicamente eficiente y técnicamente viable, todo ello sin perjuicio de que, en todo caso, deba existir una comunicación previa mínima de un mes de antelación del operador a la comunidad de propietarios o al propietario junto con una descripción de la actuación que pretende realizar, antes de iniciar cualquier instalación. En todo caso, será necesario que el operador indique a la comunidad de propietarios o al propietario el día de inicio de la instalación.

5. Los operadores serán responsables de cualquier daño que infrinjan en las edificaciones o fincas como consecuencia de las actividades de instalación de las redes y recursos asociados a que se refiere el apartado anterior.

6. Por orden del Ministerio de Industria, Energía y Turismo se determinarán los aspectos técnicos que deben cumplir los operadores en la instalación de los recursos asociados a las redes fijas de comunicaciones electrónicas de acceso ultrarrápido así como la obra civil asociada en los supuestos contemplados en el apartado 4 de este artículo, con el objetivo de reducir molestias y cargas a los ciudadanos, optimizar la instalación de las redes y facilitar el despliegue de las redes por los distintos operadores.

7. El Ministerio de Industria, Energía y Turismo podrá imponer a los operadores y a los propietarios de los correspondientes recursos asociados, previo trámite de información pública, obligaciones objetivas, transparentes, proporcionadas y no discriminatorias relativas a la utilización compartida de los tramos finales de las redes de acceso, incluyendo los que discurran por el interior de las edificaciones y conjuntos inmobiliarios, o hasta el primer punto de concentración o distribución ubicado en su exterior, cuando la duplicación de esta infraestructura sea económicamente ineficiente o físicamente inviable.

8. El Ministerio de Industria, Energía y Turismo creará y mantendrá un inventario centralizado y actualizado de todos aquellos edificios o conjuntos inmobiliarios que disponen de infraestructuras comunes de telecomunicaciones instaladas. Dicho inventario será puesto a disposición de los operadores.

CAPÍTULO V

Derechos de los usuarios finales

Artículo 46. *Derechos de los usuarios finales de servicios de comunicaciones electrónicas.*

1. Son titulares de los derechos específicos reconocidos en este Capítulo, en las condiciones establecidas en el mismo, los usuarios finales de servicios de comunicaciones electrónicas. Los operadores estarán obligados a respetar los derechos reconocidos en este Capítulo.

El reconocimiento de los derechos específicos de los usuarios finales de redes y servicios de comunicaciones electrónicas disponibles al público que efectúa este Capítulo se entiende sin perjuicio de los derechos que otorga a los consumidores el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el real decreto Legislativo 1/2007, de 16 de noviembre.

2. Las disposiciones que esta ley y su desarrollo reglamentario contiene en materia de derechos específicos de los usuarios finales de servicios de comunicaciones electrónicas, en aquellos aspectos expresamente previstos en las disposiciones del derecho de la Unión Europea de las que traigan causa, serán de aplicación preferente en caso de conflicto con las disposiciones que regulen con carácter general los derechos de los consumidores y usuarios.

Artículo 47. *Derechos específicos de los usuarios finales de redes y servicios de comunicaciones electrónicas disponibles al público.*

1. Los derechos específicos de los usuarios finales de redes y servicios de comunicaciones electrónicas se establecerán por real decreto que regulará:

a) El derecho a celebrar contratos por parte de los usuarios finales con los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público, así como el contenido mínimo de dichos contratos, sin perjuicio de lo dispuesto en el artículo 53.

b) El derecho a resolver el contrato en cualquier momento. Este derecho incluye el de resolverlo anticipadamente y sin penalización en el supuesto de modificación de las condiciones contractuales impuestas por el operador por motivos válidos especificados en aquél y sin perjuicio de otras causas de resolución unilateral.

c) El derecho al cambio de operador, con conservación de los números del plan nacional de numeración telefónica en los supuestos en que así se contemple en el plazo máximo de un día laborable. No se podrá transferir a los usuarios finales a otro operador en contra de su voluntad.

Los usuarios finales deberán recibir información adecuada sobre el cambio de operador, cuyo proceso es dirigido por el operador receptor, antes y durante el proceso, así como inmediatamente después de su conclusión.

Los contratos de los usuarios finales con los operadores cedentes, en lo relativo a los servicios afectados por la conservación de los números, quedarán automáticamente resueltos una vez concluido el proceso de cambio de operador.

El retraso en la conservación de los números y los abusos de la conservación por parte de los operadores o en su nombre, dará derecho a los abonados a una compensación en los términos que se establezcan mediante real decreto, en el que se fijarán asimismo los supuestos en que dicha compensación será automática. Las condiciones y procedimientos para la resolución de los contratos no deberán constituir un factor disuasorio para cambiar de operador.

d) El derecho a la información, que deberá ser veraz, eficaz, suficiente, transparente, comparable, sobre los servicios de comunicaciones electrónicas disponibles al público, sin perjuicio de lo dispuesto en el artículo 54.

e) Los supuestos, plazos y condiciones en que el usuario, previa solicitud, podrá ejercer el derecho de desconexión de determinados servicios, contemplándose la necesidad de petición expresa para el acceso a servicios de distinta consideración.

f) El derecho a la continuidad del servicio, y a obtener una compensación automática por su interrupción, en los supuestos que se determinen mediante real decreto.

g) Los supuestos de aprobación por parte del Ministerio de Industria, Energía y Turismo de las condiciones generales de los contratos, entre los que se incluirán los celebrados entre los usuarios finales y los operadores que exploten redes o presten servicios de comunicaciones electrónicas con obligaciones de servicio público.

La aprobación administrativa a la que se refiere el párrafo anterior no excluye el control ni administrativo ni judicial de las condiciones generales de la contratación contenidas en los citados contratos, conforme a la normativa vigente.

h) El derecho a recibir información completa, comparable, pertinente, fiable, actualizada y de fácil consulta sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público y sobre las medidas adoptadas para garantizar un acceso equivalente para los usuarios finales con discapacidad.

i) El derecho a elegir un medio de pago para el abono de los correspondientes servicios entre los comúnmente utilizados en el tráfico comercial.

j) El derecho a acceder a los servicios de emergencias de forma gratuita sin tener que utilizar ningún medio de pago.

k) El derecho a la facturación detallada, clara y sin errores, sin perjuicio del derecho a recibir facturas no desglosadas a petición del usuario.

l) El derecho a detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero.

m) El derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.

Los usuarios finales no podrán ejercer este derecho cuando se trate de llamadas de emergencia a través del número 112 o comunicaciones efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen mediante real decreto.

Por un período de tiempo limitado, los usuarios finales no podrán ejercer este derecho cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea.

n) El derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

En este supuesto y en el anterior, los operadores que presten servicios de comunicaciones electrónicas al público para efectuar llamadas nacionales a números de un plan nacional de numeración telefónica, así como los que exploten redes públicas de comunicaciones electrónicas, deberán cumplir las condiciones que mediante real decreto se determinen sobre la visualización, restricción y supresión de la identificación de la línea de origen y conectada.

2. Los operadores deberán disponer de un servicio de atención al cliente, gratuito para los usuarios, que tenga por objeto facilitar información y atender y resolver las quejas y reclamaciones de sus clientes.

Los servicios de atención al cliente mediante el canal telefónico deberán garantizar una atención personal directa, más allá de la posibilidad de utilizar complementariamente otros medios técnicos a su alcance para mejorar dicha atención. Los operadores pondrán a disposición de sus clientes métodos para la acreditación documental de las gestiones o reclamaciones realizadas, como el otorgamiento de un número de referencia o la posibilidad de enviar al cliente un documento en soporte duradero.

Artículo 48. *Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados.*

1. Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo e informado para ello.

b) A oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en la letra anterior y a ser informado de este derecho.

2. Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio, para la devolución del cargo efectuado por el operador, para el pago de la factura o para que el operador pueda exigir su pago.

b) A que sus datos de tráfico sean utilizados para promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido, en la medida y durante el tiempo necesarios para tales servicios o promoción comercial únicamente cuando hubieran prestado su consentimiento informado para ello. Los usuarios finales dispondrán del derecho de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento y con efecto inmediato.

c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico.

Los usuarios finales no podrán ejercer este derecho cuando se trate de llamadas de emergencia a través del número 112 o comunicaciones efectuadas a entidades que presten servicios de llamadas de urgencia que se determinen por el Ministerio de Industria, Energía y Turismo.

3. Respecto a la protección de datos personales y la privacidad en relación con las guías de abonados, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A figurar en las guías de abonados.

b) A ser informados gratuitamente de la inclusión de sus datos en las guías, así como de la finalidad de las mismas, con carácter previo a dicha inclusión.

c) A no figurar en las guías o a solicitar la omisión de algunos de sus datos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor.

4. Lo establecido en las letras a) y c) del apartado 2 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 49. *Guías de abonados.*

1. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia.

A tal efecto, las empresas que asignen números de teléfono a los abonados habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato aprobado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometido el suministro de la citada información y su posterior utilización a la normativa en materia de protección de datos vigente en cada momento.

El Ministerio de Industria, Energía y Turismo deberá suministrar gratuitamente a las entidades que vayan a elaborar guías telefónicas de abonados, a las que presten el servicio de consulta telefónica sobre números de abonado y a las que presten los servicios de llamadas de emergencia, los datos que le faciliten los operadores, de conformidad con las condiciones que se establezcan mediante real decreto.

2. Se garantiza el acceso de los usuarios finales a los servicios de información sobre números de abonados, para cuya consecución el Ministerio de Industria, Energía y Turismo podrá imponer obligaciones y condiciones a las empresas que controlan el acceso a los usuarios finales en materia de prestación de servicios de información sobre números de abonado que deberán ser objetivas, equitativas, no discriminatorias y transparentes.

3. El Ministerio de Industria, Energía y Turismo adoptará, siempre que sea técnica y económicamente posible, medidas para garantizar el acceso directo de los usuarios finales

al servicio de información sobre números de abonados de otro país comunitario mediante llamada vocal o SMS.

Artículo 50. *Calidad de servicio.*

1. Por Orden del Ministro de Industria, Energía y Turismo se podrán fijar requisitos mínimos de calidad de servicio que, en su caso, se exijan a los operadores de redes públicas de comunicaciones electrónicas, con objeto de evitar la degradación del servicio y la obstaculización o ralentización del tráfico en las redes, de acuerdo con los procedimientos que se establezcan mediante real decreto.

El Ministerio de Industria, Energía y Turismo facilitará a la Comisión Europea, a su debido tiempo antes de establecer tales requisitos, un resumen de los motivos para la acción, los requisitos previstos y la línea de acción propuesta. Dicha información se pondrá también a disposición del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE).

2. Asimismo, se podrán establecer los parámetros de calidad que habrán de cuantificarse, así como los posibles mecanismos de certificación de la calidad, al objeto de garantizar que los usuarios finales, incluidos los usuarios finales con discapacidad, tengan acceso a una información completa, comparable, fiable y de fácil consulta.

Artículo 51. *Acceso a números o servicios.*

1. En la medida que resulte necesario para la consecución de los objetivos establecidos en el artículo 3 y, en particular, para salvaguardar los derechos e intereses de los usuarios, mediante real decreto o en los Planes Nacionales de numeración, direccionamiento y denominación y sus disposiciones de desarrollo, podrán establecerse requisitos sobre capacidades o funcionalidades mínimas que deberán cumplir determinados tipos de servicios.

2. Asimismo, mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se establecerán las condiciones en las que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público lleven a cabo el bloqueo de acceso a números o servicios, siempre que esté justificado por motivos de tráfico no permitido y de tráfico irregular con fines fraudulentos, y los casos en que los prestadores de servicios de comunicaciones electrónicas retengan los correspondientes ingresos por interconexión u otros servicios. La Comisión Nacional de los Mercados y la Competencia podrá ordenar el bloqueo de acceso a números o servicios por motivos de tráfico irregular con fines fraudulentos cuando tengan su origen en un conflicto entre operadores en materia de acceso o interconexión que le sea planteado por dichos operadores. En ningún caso podrá exigirse al amparo de este apartado el bloqueo a servicios no incluidos en el ámbito de aplicación de esta Ley, como los servicios de la Sociedad de la Información regulados en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

3. Mediante Resolución el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información podrá establecer que, por razones de protección de los derechos de los usuarios finales de servicios de comunicaciones electrónicas, en especial, relacionadas con la facturación y las tarifas que se aplican en la prestación de determinados servicios, algunos números o rangos de numeración sólo sean accesibles previa petición expresa del usuario, en las condiciones que se fijen en dicha Resolución.

Artículo 52. *Regulación de las condiciones básicas de acceso por personas con discapacidad.*

Mediante real decreto se podrán establecer las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con las comunicaciones electrónicas. En la citada norma se establecerán los requisitos que deberán cumplir los operadores para garantizar que los usuarios con discapacidad:

a) Puedan tener un acceso a servicios de comunicaciones electrónicas equivalente al que disfrutan la mayoría de los usuarios finales.

b) Se beneficien de la posibilidad de elección de empresa y servicios disponible para la mayoría de usuarios finales.

Artículo 53. *Contratos.*

1. Antes de la celebración de un contrato entre usuarios finales y los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público, los operadores proporcionarán a los usuarios finales al menos la información que a estos efectos se establece en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

Adicionalmente a lo establecido en el párrafo anterior, los operadores también proporcionarán, antes de la celebración del contrato, la información específica sobre el servicio de comunicaciones electrónicas que se establezca mediante real decreto, y al menos:

a) Descripción de los servicios a proveer y posibles limitaciones en su uso.

b) Los precios y tarifas aplicables, con los conceptos y detalles que se establezcan mediante real decreto.

c) Duración de los contratos y causas para su resolución.

d) Información sobre restricciones impuestas en cuanto a las posibilidades de utilizar el equipo terminal suministrado.

e) Condiciones aplicables en relación con la conservación de números.

2. El contenido de los contratos que se celebren entre los usuarios finales y los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público se regulará mediante real decreto, e incluirá de forma clara, comprensible y fácilmente accesible, al menos, el siguiente contenido específico:

a) Los servicios prestados, incluyendo, en particular:

i) Si se facilita o no el acceso a los servicios de emergencia e información sobre la ubicación de las personas que efectúan la llamada, así como cualquier otra limitación para la prestación de servicios de emergencia.

ii) Información sobre cualquier otra condición que limite el acceso o la utilización de los servicios y las aplicaciones.

iii) Los niveles mínimos de calidad de servicio que se ofrecen, en particular, el plazo para la conexión inicial, así como, en su caso, otros parámetros de calidad de servicio establecidos reglamentariamente.

iv) Información sobre cualquier procedimiento establecido por la empresa para medir y gestionar el tráfico de forma que se evite agotar o saturar el enlace de la red, e información sobre la manera en que esos procedimientos pueden afectar a la calidad del servicio.

v) Los tipos de mantenimiento ofrecidos y los servicios de apoyo facilitados al cliente, así como los medios para entrar en contacto con dichos servicios.

vi) Cualquier restricción impuesta por el proveedor en cuanto a las posibilidades de utilizar el equipo terminal suministrado.

b) La decisión del abonado acerca de la posibilidad de incluir o no sus datos personales en una guía determinada y los datos de que se trate.

c) La duración del contrato y las condiciones para su renovación y para la terminación de los servicios y la resolución del contrato, incluidos:

i) Cualquier uso o duración mínimos u otros requisitos requeridos para aprovechar las promociones.

ii) Todos los gastos relacionados con la conservación del número y otros identificadores.

iii) Todos los gastos relacionados con la resolución del contrato, incluida la recuperación de costes relacionada con los equipos terminales.

iv) Las condiciones en las que en los supuestos de cambio de operador con conservación de números, el operador cedente se comprometa, en su caso, a reembolsar cualquier crédito restante en las tarjetas prepago.

d) El modo de iniciar los procedimientos de resolución de litigios, de conformidad con el artículo 55.

e) Los tipos de medidas que podría tomar la empresa en caso de incidentes de seguridad o integridad o de amenazas y vulnerabilidad.

3. Mediante real decreto podrá establecerse la obligatoriedad de que los contratos incluyan la información que determine la autoridad competente, en relación con el uso de las redes y servicios de comunicaciones electrónicas para desarrollar actividades ilícitas o para difundir contenidos nocivos, así como sobre los medios de protección frente a riesgos para la seguridad personal, la privacidad y los datos personales, siempre que sean pertinentes para el servicio prestado.

4. Los operadores deberán entregar o remitir a los usuarios por escrito o en cualquier otro soporte duradero el contrato celebrado.

Artículo 54. *Transparencia y publicación de información.*

1. Mediante real decreto se establecerán las condiciones para que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público publiquen información transparente, comparable, adecuada y actualizada sobre los precios y tarifas aplicables, y, en su caso, sobre los gastos y condiciones relacionadas con la terminación de los contratos, así como información sobre el acceso y la utilización de los servicios que prestan a los usuarios finales, que será publicada de forma clara, comprensible y fácilmente accesible.

2. El Ministerio de Industria, Energía y Turismo fomentará la divulgación de información comparable con objeto de que los usuarios finales puedan hacer una evaluación independiente del coste de las modalidades de uso alternativas, por ejemplo, mediante guías alternativas o técnicas similares, y regulará las condiciones para que la información publicada por los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público pueda ser utilizada gratuitamente por terceros, con el fin de vender o permitir la utilización de estas guías interactivas o técnicas similares.

3. Mediante real decreto se regularán las condiciones para garantizar que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público:

a) Ofrezcan a los abonados información sobre las tarifas aplicables en relación con cualquier número o servicio sujetos a condiciones de precios específicas, por lo que se refiere a cada una de las categorías de servicios, pudiéndose exigir que dicha información se facilite inmediatamente antes de efectuar las llamadas.

b) Informen a los abonados sobre todo cambio de acceso a los servicios de emergencia o a la información relativa a la ubicación de las personas que efectúan las llamadas en el servicio al que están abonados.

c) Informen a los abonados de los cambios en las condiciones que limiten el acceso o la utilización de los servicios y las aplicaciones.

d) Proporcionen información sobre cualquier procedimiento establecido por el proveedor para medir y gestionar el tráfico de forma que se evite agotar o saturar el enlace de la red y sobre la manera en que esos procedimientos pueden afectar la calidad del servicio.

e) Informen a los abonados de su derecho a decidir si incluyen sus datos personales en una guía y los tipos de datos de que se trata.

f) Informen de forma periódica y detallada a los abonados con discapacidad de los productos y servicios dirigidos a ellos.

4. El Ministerio de Industria, Energía y Turismo podrá exigir a los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público que difundan de forma gratuita, y en un determinado formato, información de interés público a los antiguos y nuevos abonados, cuando proceda, por las mismas vías utilizadas normalmente por éstos para comunicarse con los abonados, información que cubrirá los siguientes aspectos:

a) Los usos más comunes de los servicios de comunicaciones electrónicas para desarrollar actividades ilícitas o para difundir contenidos nocivos, en particular cuando ello atente contra los derechos y libertades de terceros, incluyendo las infracciones de los derechos de autor y derechos afines, así como sus consecuencias jurídicas.

b) Los medios de protección contra los riesgos para la seguridad personal, la privacidad, y los datos de carácter personal en el uso de los servicios de comunicaciones electrónicas.

5. El Ministerio de Industria, Energía y Turismo publicará periódicamente los datos resultantes de la gestión del procedimiento de resolución de controversias establecido en el apartado 1 del artículo 55. Los datos incluirán un nivel de desagregación que permita obtener información acerca de los servicios, materias y operadores sobre los que versan las reclamaciones recibidas.

Artículo 55. *Resolución de controversias.*

1. Los usuarios finales que sean personas físicas tendrán derecho a disponer de un procedimiento extrajudicial, transparente, no discriminatorio, sencillo y gratuito para resolver sus controversias con los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público, cuando tales controversias se refieran a sus derechos específicos como usuarios finales de servicios de comunicaciones electrónicas reconocidos en esta Ley y su normativa de desarrollo y de acuerdo con lo recogido en la normativa comunitaria.

A tal fin, el Ministerio de Industria, Energía y Turismo establecerá mediante orden un procedimiento conforme al cual, los usuarios finales que sean personas físicas podrán someterle dichas controversias, con arreglo a los principios establecidos en el apartado anterior. Los operadores estarán obligados a someterse al procedimiento, así como a cumplir la resolución que le ponga fin. En cualquier caso, el procedimiento que se adopte establecerá el plazo máximo en el que deberá notificarse la resolución expresa, transcurrido el cual se podrá entender desestimada la reclamación por silencio administrativo, sin perjuicio de que la Administración de telecomunicaciones tenga la obligación de resolver la reclamación de forma expresa, de acuerdo con lo establecido en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común. La resolución que se dicte podrá impugnarse ante la jurisdicción contencioso-administrativa.

2. Lo establecido en el apartado anterior se entiende sin perjuicio del derecho de los usuarios finales a someter las controversias al conocimiento de las Juntas arbitrales de consumo, de acuerdo con la legislación vigente en la materia. Si las Juntas arbitrales de consumo acuerdan conocer sobre la controversia, no será posible acudir al procedimiento del apartado anterior.

TÍTULO IV

Evaluación de la conformidad de equipos y aparatos

Artículo 56. *Normalización técnica.*

1. Mediante real decreto se podrán establecer los supuestos y condiciones en que los operadores de redes públicas y servicios de comunicaciones electrónicas disponibles al público habrán de publicar las especificaciones técnicas precisas y adecuadas de las interfaces ofrecidas en España, con anterioridad a la posibilidad de acceso público a los servicios prestados a través de dichas interfaces.

2. Mediante real decreto se determinarán las formas de elaboración, en su caso, de las especificaciones técnicas aplicables a los equipos y aparatos de telecomunicaciones, a efectos de garantizar el cumplimiento de los requisitos esenciales en los procedimientos de evaluación de conformidad y se fijarán los equipos y aparatos exceptuados de la aplicación de dicha evaluación.

En los supuestos en que la normativa lo prevea, el Ministerio de Industria, Energía y Turismo podrá aprobar especificaciones técnicas distintas de las anteriores para aparatos de telecomunicación.

Artículo 57. *Evaluación de la conformidad.*

1. Los aparatos de telecomunicación, entendiendo por tales cualquier dispositivo no excluido expresamente del real decreto que desarrolle este título que sea equipo radioeléctrico o equipo terminal de telecomunicación, o ambas cosas a la vez, deberán evaluar su conformidad con los requisitos esenciales recogidos en las disposiciones que lo determinen, ser conformes con todas las disposiciones que se establezcan e incorporar el marcado correspondiente como consecuencia de la evaluación realizada. Podrá exceptuarse de la aplicación de lo dispuesto en este título el uso de los equipos que mediante real decreto se determine, como los equipos de radioaficionados construidos por el propio usuario y no disponibles para venta en el mercado, conforme a lo dispuesto en su regulación específica.

2. Para la importación desde terceros países no pertenecientes a la Unión Europea, la puesta en el mercado, la puesta en servicio y la utilización de un aparato de telecomunicaciones de los indicados en el apartado anterior será requisito imprescindible que el agente económico establecido en la Unión Europea o el usuario de éste haya verificado previamente la conformidad de los aparatos con los requisitos esenciales que les sean aplicables mediante los procedimientos que se determinen en el real decreto que se establezca al efecto, así como el cumplimiento de las disposiciones que se dicten en el mismo.

3. El cumplimiento de todos los requisitos que se establezcan en el real decreto indicado incluye la habilitación para la conexión de los aparatos destinados a conectarse a los puntos de terminación de una red pública de comunicaciones electrónicas. Dicho cumplimiento no supone autorización de uso para los equipos radioeléctricos sujetos a la obtención de autorización o concesión de dominio público radioeléctrico en los términos establecidos en esta Ley.

4. El Ministerio de Industria, Energía y Turismo podrá promover procedimientos complementarios de certificación voluntaria para los aparatos de telecomunicación que incluirán, al menos, la evaluación de la conformidad indicada en los capítulos anteriores.

5. El Ministerio de Industria, Energía y Turismo podrá realizar los controles adecuados para asegurar que los equipos puestos en el mercado han evaluado su conformidad de acuerdo con lo dispuesto en este título. La persona física o jurídica responsable de los equipos puestos en el mercado facilitará de manera gratuita la puesta a disposición de los equipos para poder llevar a cabo dichos controles.

Mediante real decreto se establecerá el procedimiento aplicable a la retirada del mercado de productos que incumplan lo dispuesto en este título.

Artículo 58. *Reconocimiento mutuo.*

1. Los aparatos de telecomunicación que hayan evaluado su conformidad con los requisitos esenciales en otro Estado miembro de la Unión Europea o en virtud de los acuerdos de reconocimiento mutuo celebrados por ella con terceros países, y cumplan con las demás disposiciones aplicables en la materia, tendrán la misma consideración, en lo que se refiere a lo dispuesto en este Título IV, que los aparatos cuya conformidad se ha verificado en España y cumplan, asimismo, las demás disposiciones legales en la materia.

2. El Ministerio de Industria, Energía y Turismo establecerá los procedimientos para el reconocimiento de la conformidad de los aparatos de telecomunicación a los que se refieren los acuerdos de reconocimiento mutuo que establezca la Unión Europea con terceros países.

3. Los aparatos de telecomunicación que utilicen el espectro radioeléctrico con parámetros de radio no armonizados en la Unión Europea no podrán ser puestos en el mercado mientras no hayan sido autorizados por el Ministerio de Industria, Energía y Turismo, además de haber evaluado la conformidad con las normas aplicables a aquéllos y ser conformes con el resto de disposiciones que les sean aplicables.

Artículo 59. *Condiciones que deben cumplir las instalaciones e instaladores.*

1. La instalación de los aparatos de telecomunicación deberá ser realizada siguiendo las instrucciones proporcionadas por el agente económico, manteniendo, en cualquier caso, inalteradas las condiciones bajo las cuales se ha verificado su conformidad con los requisitos esenciales, en los términos establecidos en los artículos anteriores de este título.

2. La prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta Ley y su normativa de desarrollo.

Podrán prestar servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

Mediante real decreto se establecerán los requisitos exigibles para el ejercicio de la actividad consistente en la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación relativos a la capacidad técnica y a la cualificación profesional para el ejercicio de la actividad, medios técnicos y cobertura mínima del seguro, aval o de cualquier otra garantía financiera. Los requisitos de acceso a la actividad y su ejercicio serán proporcionados, no discriminatorios, transparentes y objetivos, y estarán clara y directamente vinculados al interés general concreto que los justifique.

Los interesados en la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación deberán, con anterioridad al inicio de la actividad, presentar al Registro de empresas instaladoras de telecomunicación, por medios electrónicos o telemáticos, una declaración responsable sobre el cumplimiento de los requisitos exigibles para el ejercicio de la actividad.

La declaración responsable habilita para la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación en todo el territorio español y con una duración indefinida.

Cuando se constate el incumplimiento de alguno de los requisitos determinados reglamentariamente, se le dirigirá al interesado una notificación para que subsane dicho incumplimiento en el plazo de quince días. Transcurrido dicho plazo sin que la subsanación se hubiera producido, se procederá a dictar resolución privando de eficacia a la declaración y se cancelará la inscripción registral.

Cualquier hecho que suponga modificación de alguno de los datos incluidos en la declaración originaria deberá ser comunicado por el interesado por medios electrónicos o telemáticos, en el plazo máximo de un mes a partir del momento en que se produzca, a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, que procederá a la inscripción de la modificación en el Registro de empresas instaladoras de telecomunicación.

Si como consecuencia de la prestación de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se pusiera en peligro la seguridad de las personas o de las redes públicas de telecomunicaciones, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá dictar resolución motivada por la que, previa audiencia del interesado, se adopte de forma cautelar e inmediata y por el tiempo imprescindible para ello la suspensión del ejercicio de la actividad de instalación para el interesado, sin perjuicio de que se pueda incoar el oportuno expediente sancionador de conformidad con lo establecido en el Título VIII.

Será libre la prestación temporal u ocasional en el territorio español de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación por personas físicas o jurídicas legalmente establecidas en otros Estados miembros de la Unión Europea para el ejercicio de la misma actividad, sin perjuicio del cumplimiento de las obligaciones en materia de reconocimiento de cualificaciones profesionales que sean de aplicación a los profesionales que se desplacen.

3. El Registro de empresas instaladoras de telecomunicación será de carácter público y su regulación se hará mediante real decreto. En él se inscribirán de oficio los datos relativos

a las personas físicas o jurídicas que hayan declarado su intención de prestar servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación y sus modificaciones, a partir de la información contenida en las declaraciones. Los trámites relativos a la inscripción en el mismo no podrán suponer un retraso de la habilitación para ejercer la actividad.

TÍTULO V

Dominio público radioeléctrico

Artículo 60. *De la administración del dominio público radioeléctrico.*

1. El espectro radioeléctrico es un bien de dominio público, cuya titularidad y administración corresponden al Estado. Dicha administración se ejercerá de conformidad con lo dispuesto en este título y en los tratados y acuerdos internacionales en los que España sea parte, atendiendo a la normativa aplicable en la Unión Europea y a las resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales.

2. La administración del dominio público radioeléctrico se llevará a cabo teniendo en cuenta su importante valor social, cultural y económico y la necesaria cooperación con otros Estados miembros de la Unión Europea y con la Comisión Europea en la planificación estratégica, la coordinación y la armonización del uso del espectro radioeléctrico en la Unión Europea.

En el marco de dicha cooperación se fomentará la coordinación de los enfoques políticos en materia de espectro radioeléctrico en la Unión Europea y, cuando proceda, la armonización de las condiciones necesarias para la creación y el funcionamiento del mercado interior de las comunicaciones electrónicas. Para ello, se tendrán en cuenta, entre otros, los aspectos económicos, de seguridad, de salud, de interés público, de libertad de expresión, culturales, científicos, sociales y técnicos de las políticas de la Unión Europea, así como los diversos intereses de las comunidades de usuarios del espectro, atendiendo siempre a la necesidad de garantizar un uso eficiente y efectivo de las radiofrecuencias y a los beneficios para los consumidores, como la realización de economías de escala y la interoperabilidad de los servicios.

3. En particular, son principios aplicables a la administración del dominio público radioeléctrico, entre otros, los siguientes:

a) Garantizar un uso eficaz y eficiente de este recurso.

b) Fomentar la neutralidad tecnológica y de los servicios, y el mercado secundario del espectro.

c) Fomentar una mayor competencia en el mercado de las comunicaciones electrónicas.

4. La administración del dominio público radioeléctrico tiene por objetivo el establecimiento de un marco jurídico que asegure unas condiciones armonizadas para su uso y que permita su disponibilidad y uso eficiente, y abarca un conjunto de actuaciones entre las cuales se incluyen las siguientes:

a) Planificación: Elaboración y aprobación de los planes de utilización.

b) Gestión: Establecimiento, de acuerdo con la planificación previa, de las condiciones técnicas de explotación y otorgamiento de los derechos de uso.

c) Control: Comprobación técnica de las emisiones, detección y eliminación de interferencias, inspección técnica de instalaciones, equipos y aparatos radioeléctricos, así como el control de la puesta en el mercado de éstos últimos.

Igualmente, incluye la protección del dominio público radioeléctrico, consistente, entre otras actuaciones, en la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados, con independencia de que dichas frecuencias o canales radioeléctricos sean objeto en la práctica de ocupación o uso efectivo.

d) Aplicación del régimen sancionador.

5. La utilización de frecuencias radioeléctricas mediante redes de satélites se incluye dentro de la administración del dominio público radioeléctrico.

Asimismo, la utilización del dominio público radioeléctrico necesaria para la utilización de los recursos órbita-espectro en el ámbito de la soberanía española y mediante satélites de comunicaciones queda reservada al Estado. Su explotación estará sometida al derecho internacional y se realizará, en la forma que mediante real decreto se determine, mediante su gestión directa por el Estado o mediante concesión. En todo caso, la gestión podrá también llevarse a cabo mediante conciertos con organismos internacionales.

Artículo 61. *Facultades del Gobierno para la administración del dominio público radioeléctrico.*

El Gobierno desarrollará mediante real decreto las condiciones para la adecuada administración del dominio público radioeléctrico. En dicho real decreto se regulará, como mínimo, lo siguiente:

a) El procedimiento para la elaboración de los planes de utilización del espectro radioeléctrico, que incluyen el Cuadro Nacional de Atribución de Frecuencias, los planes técnicos nacionales de radiodifusión y televisión, cuya aprobación corresponderá al Gobierno, y las necesidades de espectro radioeléctrico para la defensa nacional. Los datos relativos a esta última materia tendrán el carácter de reservados.

b) El procedimiento de determinación, control e inspección de los niveles únicos de emisión radioeléctrica tolerable y que no supongan un peligro para la salud pública, que deberán ser respetados en todo caso y momento por las diferentes instalaciones o infraestructuras a instalar y ya instaladas que hagan uso del dominio público radioeléctrico. En la determinación de estos niveles únicos de emisión radioeléctrica tolerable se tendrá en cuenta tanto criterios técnicos en el uso del dominio público radioeléctrico, como criterios de preservación de la salud de las personas, y en concordancia con lo dispuesto por las recomendaciones de la Comisión Europea. Tales límites deberán ser respetados, en todo caso, por el resto de administraciones públicas, tanto autonómicas como locales.

c) Los procedimientos, plazos y condiciones para la habilitación del ejercicio de los derechos de uso del dominio público radioeléctrico, que revestirá la forma de autorización general, autorización individual, afectación o concesión administrativas.

En particular, se regularán los procedimientos abiertos de otorgamiento de derechos de uso del dominio público radioeléctrico, que se basarán en criterios objetivos, transparentes, no discriminatorios y proporcionados y tendrán en cuenta, entre otras circunstancias, la tecnología utilizada, el interés de los servicios, las bandas y su grado de aprovechamiento. También tendrán en consideración la valoración económica para el interesado del uso del dominio público, dado que éste es un recurso escaso y, en su caso, las ofertas presentadas por los licitadores.

No obstante lo anterior, cuando resulte necesario el otorgamiento de derechos individuales de utilización de radiofrecuencias a proveedores de servicios de contenidos radiofónicos o televisivos para lograr un objetivo de interés general establecido de conformidad con el Derecho de la Unión Europea, podrán establecerse excepciones al requisito de procedimiento abierto.

d) El procedimiento para la reasignación del uso de bandas de frecuencias con el objetivo de alcanzar un uso más eficiente del espectro radioeléctrico, en función de su idoneidad para la prestación de nuevos servicios o de la evaluación de las tecnologías, que podrá incluir el calendario de actuaciones y la evaluación de los costes asociados, en particular, los ocasionados a los titulares de derechos de uso afectados por estas actuaciones de reasignación, que podrán verse compensados a través de un fondo económico o cualquier otro mecanismo de compensación que se establezca.

e) Las condiciones no discriminatorias, proporcionadas y transparentes asociadas a los títulos habilitantes para el uso del dominio público radioeléctrico, entre las que se incluirán las necesarias para garantizar el uso efectivo y eficiente de las frecuencias y los compromisos contraídos por los operadores en los procesos de licitación previstos en el artículo 63. Estas condiciones buscarán promover en todo caso la consecución de los

mayores beneficios posibles para los usuarios, así como mantener los incentivos suficientes para la inversión y la innovación.

f) Las condiciones de otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico para fines experimentales o eventos de corta duración.

g) La adecuada utilización del espectro radioeléctrico mediante el empleo de equipos y aparatos.

Artículo 62. *Títulos habilitantes para el uso del dominio público radioeléctrico.*

1. El uso del dominio público radioeléctrico podrá ser común, especial o privativo.

El uso común del dominio público radioeléctrico no precisará de ningún título habilitante y se llevará a cabo en las bandas de frecuencias y con las características técnicas que se establezcan al efecto.

El uso especial del dominio público radioeléctrico es el que se lleve a cabo de las bandas de frecuencias habilitadas para su explotación de forma compartida, sin limitación de número de operadores o usuarios y con las condiciones técnicas y para los servicios que se establezcan en cada caso.

El uso privativo del dominio público radioeléctrico es el que se realiza mediante la explotación en exclusiva o por un número limitado de usuarios de determinadas frecuencias en un mismo ámbito físico de aplicación.

2. Los títulos habilitantes mediante los que se otorguen derechos de uso del dominio público radioeléctrico revestirán la forma de autorización general, autorización individual, afectación o concesión administrativas. El plazo para el otorgamiento de los títulos habilitantes será de seis semanas desde la entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, sin perjuicio de lo establecido para los derechos de uso con limitación de número. Dicho plazo no será de aplicación cuando sea necesaria la coordinación internacional de frecuencias o afecte a reservas de posiciones orbitales.

3. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización general en los supuestos de uso especial de las bandas de frecuencia habilitadas a tal efecto a través de redes públicas de comunicaciones electrónicas instaladas o explotadas por operadores de comunicaciones electrónicas.

La autorización general se entenderá concedida sin más trámite que la notificación a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, mediante el procedimiento y con los requisitos que se establezcan mediante orden del Ministerio de Industria, Energía y Turismo, sin perjuicio de la obligación de abono de las tasas correspondientes. Cuando dicha Secretaría de Estado constate que la notificación no reúne los requisitos establecidos anteriormente, dictará resolución motivada en un plazo máximo de 15 días, no teniendo por realizada aquélla.

4. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización individual en los siguientes supuestos:

a) Si se trata de una reserva de derecho de uso especial por radioaficionados u otros sin contenido económico en cuya regulación específica así se establezca.

b) Si se otorga el derecho de uso privativo para autoprestación por el solicitante, salvo en el caso de administraciones públicas, que requerirán de afectación demanial.

5. En el resto de supuestos no contemplados en los apartados anteriores, el derecho al uso privativo del dominio público radioeléctrico requerirá una concesión administrativa. Para el otorgamiento de dicha concesión, será requisito previo que los solicitantes ostenten la condición de operador de comunicaciones electrónicas y que en ellos no concurra alguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado por el real decreto Legislativo 3/2011, de 14 de noviembre.

Las concesiones de uso privativo del dominio público radioeléctrico reservado para la prestación de servicios audiovisuales se otorgará por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aneja al título habilitante audiovisual. La duración de estas concesiones será la del título habilitante audiovisual. En estos supuestos, el operador en cuyo favor se otorgue la concesión no tiene por qué ostentar

la condición de operador de comunicaciones electrónicas sino la de prestador de servicios audiovisuales.

6. Es competencia de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información el otorgamiento de los títulos habilitantes salvo en los supuestos de otorgamiento por procedimiento de licitación contemplado en el artículo 63.

Las resoluciones mediante las cuales se otorguen las concesiones de dominio público radioeléctrico se dictarán en la forma y plazos que se establezcan mediante real decreto que establecerá, asimismo, la información que se hará pública sobre dichas concesiones.

7. Quienes resultasen seleccionados para la prestación de servicios de comunicaciones electrónicas armonizados en procedimientos de licitación convocados por las instituciones de la Unión Europea en los que se establezca la reserva a su favor de derechos de uso del dominio público radioeléctrico, se inscribirán de oficio en el Registro de operadores. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información otorgará la concesión demanial a los operadores antes mencionados. En las citadas concesiones se incluirán, entre otras, las condiciones que proceda establecidas en los procedimientos de licitación, así como los compromisos adquiridos por el operador en dicho procedimiento.

8. En el Cuadro Nacional de Atribución de Frecuencias o en los pliegos reguladores de los procedimientos de licitación para el otorgamiento de títulos habilitantes se podrán establecer cautelas para evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico, en particular mediante la fijación de límites en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial o la fijación de plazos estrictos para la explotación de los derechos de uso por parte de su titular. A tal efecto, el Ministerio de Industria, Energía y Turismo podrá adoptar medidas tales como ordenar la venta o la cesión de derechos de uso de radiofrecuencias. Estas cautelas se establecerán y aplicarán de manera que sean proporcionadas, no discriminatorias y transparentes.

9. Con carácter previo a la utilización del dominio público radioeléctrico, se exigirá, preceptivamente, la aprobación del proyecto técnico y la inspección o el reconocimiento favorable de las instalaciones por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, con el fin de comprobar que se ajustan a las condiciones previamente autorizadas.

En función de la naturaleza del servicio, de la banda de frecuencias empleada, de la importancia técnica de las instalaciones que se utilicen o por razones de eficacia en la gestión del espectro, podrá sustituirse la aprobación del proyecto técnico por una declaración responsable de conformidad con lo establecido en el artículo 71 bis de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común, sin perjuicio de que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información pueda exigir en cualquier momento la presentación del proyecto técnico. Asimismo, podrá acordarse la sustitución de la inspección previa por una certificación expedida por técnico competente.

10. Los operadores que exploten las redes o servicios de comunicaciones electrónicas que hagan uso del dominio público radioeléctrico deberán disponer del correspondiente título habilitante de dicho uso.

Los operadores que vayan a efectuar materialmente emisiones radioeléctricas mediante el uso del dominio público radioeléctrico por encargo de otras personas o entidades deberán verificar, previamente al inicio de dichas emisiones, que las entidades a cuya disposición ponen su red ostentan el correspondiente título habilitante en materia de uso del dominio público radioeléctrico. Dichos operadores no podrán poner a disposición de las entidades referidas su red y, en consecuencia, no podrán dar el acceso a su red a dichas entidades ni podrán efectuar las mencionadas emisiones en caso de ausencia del citado título habilitante.

Artículo 63. *Títulos habilitantes otorgados mediante un procedimiento de licitación.*

1. Cuando sea preciso para garantizar el uso eficaz y eficiente del espectro radioeléctrico, teniendo debidamente en cuenta la necesidad de conseguir los máximos beneficios para los usuarios y facilitar el desarrollo de la competencia, el Ministerio de Industria, Energía y Turismo podrá, previa audiencia a las partes interesadas, incluidas las asociaciones de consumidores y usuarios, limitar el número de concesiones demaniales a

otorgar sobre dicho dominio para la explotación de redes públicas y la prestación de servicios de comunicaciones electrónicas. Toda decisión de limitar el otorgamiento de derechos de uso habrá de ser publicada, exponiendo los motivos de la misma. La limitación del número de títulos habilitantes será revisable por el propio Ministerio, de oficio o a instancia de parte, en la medida en que desaparezcan las causas que la motivaron.

2. Cuando, de conformidad con lo previsto en el apartado anterior, el Ministro de Industria, Energía y Turismo limite el número de concesiones demaniales a otorgar en una determinada banda de frecuencias, se tramitará un procedimiento de licitación para el otorgamiento de las mismas que respetará en todo caso los principios de publicidad, concurrencia y no discriminación para todas las partes interesadas. Para ello se aprobará, mediante orden del Ministro de Industria, Energía y Turismo, la convocatoria y el pliego de bases por el que se regirá la licitación.

El procedimiento de licitación deberá resolverse mediante orden del Ministro de Industria, Energía y Turismo en un plazo máximo de ocho meses desde la convocatoria de la licitación.

Artículo 64. *Duración, modificación, extinción y revocación de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Los derechos de uso privativo del dominio público radioeléctrico sin limitación de número se otorgarán, con carácter general, por un período que finalizará el 31 de diciembre del año natural en que cumplan su quinto año de vigencia, renovables por períodos de cinco años en función de las disponibilidades y previsiones de la planificación de dicho dominio público. Mediante real decreto se determinarán los supuestos en los que podrá fijarse un período de duración distinto para los derechos de uso privativo del dominio público radioeléctrico sin limitación de número.

2. Los derechos de uso privativo con limitación de número tendrán la duración prevista en los correspondientes procedimientos de licitación que, en todo caso, será de un máximo de veinte años, incluyendo posibles prórrogas y sin posibilidad de renovación automática. A la hora de determinar en el procedimiento de licitación la duración concreta de los derechos de uso, se tendrán en cuenta, entre otros criterios, las inversiones que se exijan y los plazos para su amortización, las obligaciones vinculadas a los derechos de uso, como la cobertura mínima que se imponga, y las bandas de frecuencias cuyos derechos de uso se otorguen, en los términos que se concreten mediante real decreto.

3. Con arreglo a los principios de objetividad y de proporcionalidad, atendiendo principalmente a las necesidades de la planificación y del uso eficiente y a la disponibilidad del espectro radioeléctrico, en los términos establecidos mediante real decreto, el Ministerio de Industria, Energía y Turismo podrá modificar los títulos habilitantes para el uso del dominio público radioeléctrico, previa audiencia del interesado.

Cuando los títulos hubiesen sido otorgados por el procedimiento de licitación se requerirá, además, informe previo de la Comisión Nacional de los Mercados y de Competencia y audiencia del Consejo de Consumidores y Usuarios y, en su caso, de las asociaciones más representativas de los restantes usuarios durante un plazo suficiente, que salvo en circunstancias excepcionales no podrá ser inferior a cuatro semanas. En estos casos la modificación se realizará mediante orden ministerial, previo informe de la Comisión Delegada del Gobierno para Asuntos Económicos, que establecerá un plazo para que los titulares se adapten a ella.

La modificación de los títulos habilitantes para el uso del dominio público radioeléctrico, en los casos en que justificadamente haya que establecer condiciones distintas a las que existían cuando se otorgó el título, podrá consistir en prolongar la duración de derechos ya existentes, incluso más allá de las duraciones establecidas en los apartados anteriores.

4. Los títulos habilitantes para el uso del dominio público se extinguirán por:

a) Las causas que resulten aplicables de las reseñadas en el artículo 100 de la Ley 33/2003, de 3 de noviembre, de Patrimonio de las administraciones públicas.

b) Muerte del titular del derecho de uso del dominio público radioeléctrico o extinción de la persona jurídica titular.

c) Renuncia del titular, con efectos desde su aceptación por el órgano competente del Ministerio de Industria, Energía y Turismo.

d) Pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico, cuando dicha condición fuera necesaria, o cualquier causa que imposibilite la prestación del servicio por su titular.

e) Falta de pago de la tasa por reserva del dominio público radioeléctrico.

f) Pérdida de adecuación de las características técnicas de la red al Cuadro Nacional de Atribución de Frecuencias, sin que exista posibilidad de otorgar al titular otras bandas.

g) Mutuo acuerdo entre el titular y el órgano competente del Ministerio de Industria, Energía y Turismo.

h) Transcurso del tiempo para el que se otorgaron. En el caso de los derechos de uso sin limitación de número, por el transcurso del tiempo para el que se otorgaron sin que se haya efectuado su renovación.

i) Por incumplimiento grave y reiterado de las obligaciones del titular contempladas como causa de revocación.

j) Aquellas otras causas que se establezcan en el título habilitante, conforme a la presente Ley.

5. El órgano competente del Ministerio de Industria, Energía y Turismo, a través del procedimiento administrativo general de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común, podrá acordar la revocación de los títulos habilitantes para el uso del dominio público radioeléctrico por las siguientes causas:

a) El incumplimiento de las condiciones y requisitos técnicos aplicables al uso del dominio público radioeléctrico.

b) No pagar el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados.

c) No efectuar un uso eficaz o eficiente del dominio público radioeléctrico.

d) La revocación sucesiva de dos autorizaciones administrativas de transferencia de título o de cesión de derechos de uso del dominio público radioeléctrico sobre el mismo título habilitante en el plazo de un año.

e) La utilización de las frecuencias con fines distintos a los que motivaron su asignación o para otros diferentes de los de la prestación del servicio o el ejercicio de la actividad que haya motivado su asignación.

Artículo 65. *Protección activa del dominio público radioeléctrico.*

1. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, en cualquier momento, podrá efectuar una protección activa del dominio público radioeléctrico mediante la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados.

Esta potestad se ejercitará sin perjuicio de las actuaciones inspectoras y sancionadoras que se puedan llevar a cabo para depurar las responsabilidades en que se hubieran podido incurrir por el uso del dominio público radioeléctrico sin disponer de título habilitante, por la producción de interferencias perjudiciales o por la comisión de cualquier otra infracción tipificada en el marco del régimen sancionador establecido en el Título VIII de esta Ley.

2. Mediante real decreto se regulará el procedimiento para el ejercicio de la potestad de protección activa del dominio público radioeléctrico en el caso de que la frecuencia o canal radioeléctrico sea objeto de una ocupación o uso efectivo sin que se disponga de título habilitante, con sujeción a las siguientes normas:

a) Se constatará la ocupación o uso efectivo de la frecuencia o canal radioeléctrico sin que se disponga de título habilitante para ello.

b) Se efectuará un trámite de previa audiencia a la persona física o jurídica que esté efectuando la ocupación o el uso de la frecuencia o canal radioeléctrico sin título habilitante o, en su caso, al titular de las infraestructuras, de la finca o del inmueble desde donde se produce la emisión en esa frecuencia, para que en el plazo de 10 días hábiles alegue lo que estime oportuno.

c) En su caso, una vez efectuado el trámite de previa audiencia, se requerirá a la persona o titular mencionado anteriormente con el que se evacuó dicho trámite, para que en el plazo de 8 días hábiles proceda al cese de las emisiones no autorizadas.

d) En el caso de que no se proceda al cese de las emisiones no autorizadas, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá iniciar sus emisiones en dicha frecuencia o canal radioeléctrico.

Artículo 66. *Neutralidad tecnológica y de servicios en el uso del dominio público radioeléctrico.*

1. En las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de Frecuencias se podrá emplear cualquier tipo de tecnología utilizada para los servicios de comunicaciones electrónicas de conformidad con el Derecho de la Unión Europea.

Podrán, no obstante, preverse restricciones proporcionadas y no discriminatorias a los tipos de tecnología de acceso inalámbrico o red radioeléctrica utilizados para los servicios de comunicaciones electrónicas cuando sea necesario para:

a) Evitar interferencias perjudiciales.
b) Proteger la salud pública frente a los campos electromagnéticos.
c) Asegurar la calidad técnica del servicio.
d) Garantizar un uso compartido máximo de las radiofrecuencias.
e) Garantizar un uso eficiente del espectro.
f) Garantizar el logro de un objetivo de interés general.

2. En las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de Frecuencias se podrá prestar cualquier tipo de servicios de comunicaciones electrónicas, de conformidad con el Derecho de la Unión Europea.

Podrán, no obstante, preverse restricciones proporcionadas y no discriminatorias a los tipos de servicios de comunicaciones electrónicas que se presten, incluido, cuando proceda, el cumplimiento de un requisito del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones.

Las medidas que exijan que un servicio de comunicaciones electrónicas se preste en una banda específica disponible para los servicios de comunicaciones electrónicas deberán estar justificadas para garantizar el logro de objetivos de interés general definidos con arreglo al Derecho de la Unión Europea, tales como:

a) La seguridad de la vida.
b) La promoción de la cohesión social, regional o territorial.
c) La evitación del uso ineficiente de las radiofrecuencias.
d) La promoción de la diversidad cultural y lingüística y del pluralismo de los medios de comunicación, mediante, por ejemplo, la prestación de servicios de radiodifusión y televisión.

Únicamente se impondrá la atribución específica de una banda de frecuencias para la prestación de un determinado servicio de comunicaciones electrónicas cuando esté justificado por la necesidad de proteger servicios relacionados con la seguridad de la vida o, excepcionalmente, cuando sea necesario para alcanzar objetivos de interés general definidos con arreglo al Derecho de la Unión Europea.

3. Las restricciones a la utilización de bandas de frecuencias que, en su caso, se establezcan de conformidad con los apartados anteriores sólo podrán adoptarse tras haber dado a las partes interesadas la oportunidad de formular observaciones sobre la medida propuesta, en un plazo razonable.

4. Periódicamente, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información revisará la pertinencia de mantener las restricciones a la utilización de bandas de frecuencias que, en su caso, se establezcan de conformidad con los apartados anteriores, hará públicos los resultados de estas revisiones y elevará las propuestas correspondientes al órgano competente para su aprobación.

Artículo 67. *Mercado secundario en el dominio público radioeléctrico.*

1. Los títulos habilitantes de uso del dominio público radioeléctrico podrán ser transferidos y los derechos de uso del dominio público radioeléctrico podrán ser cedidos, ya sea de forma total o parcial, en las condiciones de autorización que se establezcan mediante real decreto.

En dicho real decreto se identificarán igualmente las bandas de frecuencia en las que se pueden efectuar operaciones de transferencia de títulos o cesión de derechos de uso de dominio público radioeléctrico, en particular, las bandas de frecuencias que en su caso se identifiquen en el ámbito de la Unión Europea.

2. En el caso de la cesión total o parcial, ésta en ningún caso eximirá al titular del derecho de uso cedente de las obligaciones asumidas frente a la Administración. Cualquier transferencia de título habilitante o cesión de derechos de uso del dominio público radioeléctrico deberá en todo caso respetar las condiciones técnicas de uso establecidas en el Cuadro Nacional de Atribución de Frecuencias o en los planes técnicos o las que, en su caso, estén fijadas en las medidas técnicas de aplicación de la Unión Europea.

3. Mediante real decreto se establecerán las restricciones a la transferencia o arrendamiento de derechos individuales de uso de radiofrecuencias cuando dichos derechos se hubieran obtenido inicialmente de forma gratuita.

TÍTULO VI

La administración de las telecomunicaciones

Artículo 68. *Competencias de la Administración General del Estado y de sus organismos públicos.*

1. Tendrán la consideración de Autoridad Nacional de Reglamentación de Telecomunicaciones:

a) El Gobierno.

b) Los órganos superiores y directivos del Ministerio de Industria, Energía y Turismo que, de conformidad con la estructura orgánica del departamento, asuman las competencias asignadas a este ministerio en materias reguladas por esta Ley.

c) Los órganos superiores y directivos del Ministerio de Economía y Competitividad que, de conformidad con la estructura orgánica del departamento, asuman las competencias asignadas a este ministerio en materias reguladas por esta Ley.

d) La Comisión Nacional de los Mercados y la Competencia en el ejercicio de las competencias que se le ha asignado en materias reguladas por esta Ley.

2. En el desarrollo de las competencias que tengan encomendadas, las autoridades nacionales de reglamentación a las que se refiere el apartado 1 cooperarán mutuamente, con los restantes órganos de control de otros Estados y con los organismos pertinentes de la Unión Europea, a fin de fomentar la aplicación coherente de la normativa comunitaria en materia de comunicaciones electrónicas y contribuir al desarrollo del mercado interior. Con tal fin, apoyarán activamente los objetivos de la Comisión y del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) de promover una mayor coordinación. Asimismo colaborarán con ambas instituciones, a fin de determinar qué tipos de instrumentos y soluciones son los más apropiados para tratar situaciones particulares de mercado.

3. En el desarrollo de las competencias que tengan encomendadas las autoridades nacionales de reglamentación a las que se refiere el apartado 1, aplicarán principios reguladores objetivos, transparentes, no discriminatorios y proporcionados, con arreglo a los siguientes fines y criterios:

a) Promover un entorno regulador previsible, garantizando un enfoque regulador coherente en períodos de revisión apropiados.

b) Fomentar la inversión eficiente orientada al mercado y la innovación en infraestructuras nuevas y mejoradas, incluso asegurando que toda obligación relativa al acceso tenga debidamente en cuenta los riesgos en que incurren las empresas inversoras, y permitir diferentes modalidades de cooperación entre los inversores y las partes que soliciten el acceso, con el fin de diversificar el riesgo de las inversiones y velar por que se respeten la competencia en el mercado y el principio de no discriminación.

c) Imponer obligaciones específicas únicamente cuando no exista una competencia efectiva y sostenible, y suprimir dichas obligaciones en cuanto se constate el cumplimiento de dicha condición.

d) Garantizar que, en circunstancias similares, no se dispense un trato discriminatorio a las empresas suministradoras de redes y servicios de comunicaciones electrónicas.

e) Salvaguardar la competencia en beneficio de los consumidores y promover, cuando sea posible, la competencia basada en las infraestructuras.

f) Tener debidamente en cuenta la variedad de condiciones en cuanto a la competencia y los consumidores que existen en las distintas regiones geográficas.

g) Ejercer sus responsabilidades de tal modo que se promueva la eficiencia, la competencia sostenible y el máximo beneficio para los usuarios finales.

Artículo 69. *Ministerio de Industria, Energía y Turismo.*

Los órganos superiores y directivos del Ministerio de Industria, Energía y Turismo que, de conformidad con la estructura orgánica del departamento, asuman las competencias asignadas a este ministerio, ejercerán las siguientes funciones:

a) Ejecutar la política adoptada por el Gobierno en los servicios de telecomunicaciones para la defensa nacional y la protección civil a los que se refiere el artículo 4 de la presente Ley.

b) Gestionar el Registro de Operadores.

c) Ejercer las competencias que en materia de acceso a las redes y recursos asociados, interoperabilidad e interconexión le atribuye la presente Ley y su desarrollo reglamentario, en particular, en los siguientes supuestos:

1. En los procedimientos de licitación para la obtención de derechos de uso del dominio público radioeléctrico.

2. Cuando se haga necesario para garantizar el cumplimiento de la normativa sobre datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas.

3. Cuando resulte preciso para garantizar el cumplimiento de compromisos internacionales en materia de telecomunicaciones.

d) Proponer al Gobierno la aprobación de los planes nacionales de numeración, direccionamiento y denominación, el otorgamiento de los derechos de uso de los recursos públicos regulados en dichos planes y ejercer las demás competencias que le atribuye el capítulo V del Título II de la presente Ley.

e) Proponer al Gobierno la política a seguir para facilitar el desarrollo y la evolución de las obligaciones de servicio público a las que se hace referencia en el capítulo I del Título III y la desarrollará asumiendo la competencia de control y seguimiento de las obligaciones de servicio público que correspondan a los distintos operadores en la explotación de redes o la prestación de servicios de comunicaciones electrónicas.

f) Proponer al Gobierno la política a seguir para reconocer y garantizar los derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas así como los derechos de los usuarios finales a los que se hace referencia en los capítulos II, III y V del Título III.

g) Gestionar el Registro de empresas instaladoras de telecomunicación.

h) Formular las propuestas para la elaboración de normativa relativa a las infraestructuras comunes de comunicaciones electrónicas en el interior de edificios y conjuntos inmobiliarios, y el seguimiento de su implantación en España.

i) Ejercer las funciones en materia de la evaluación de la conformidad de equipos y aparatos a las que se refiere el Título IV.

j) Ejercer las funciones en materia de administración del dominio público radioeléctrico a las que se refiere el Título V. En particular, ejercerá las siguientes funciones:

1. La propuesta de planificación, la gestión y el control del dominio público radioeléctrico, así como la tramitación y el otorgamiento de los títulos habilitantes para su utilización.
2. El ejercicio de las funciones atribuidas a la Administración General del Estado en materia de autorización e inspección de instalaciones radioeléctricas en relación con los niveles únicos de emisión radioeléctrica permitidos a que se refiere el artículo 61 de esta Ley.
3. La gestión de un registro público de radiofrecuencias, accesible a través de Internet, en el que constarán los titulares de concesiones administrativas para el uso privativo del dominio público radioeléctrico.
4. La elaboración de proyectos y desarrollo de los planes técnicos nacionales de radiodifusión y televisión.
5. La comprobación técnica de emisiones radioeléctricas para la identificación, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicación, y la verificación del uso efectivo y eficiente del dominio público radioeléctrico por parte de los titulares de derechos de uso.
6. La protección del dominio público radioeléctrico, para lo cual podrá, entre otras actuaciones, realizar emisiones en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados.
7. La gestión de la asignación de los recursos órbita-espectro para comunicaciones por satélite.
8. La elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la administración del dominio público radioeléctrico.
9. La participación en los organismos internacionales relacionados con la planificación del espectro radioeléctrico.

k) Gestionar en período voluntario las tasas en materia de telecomunicaciones a que se refiere la presente Ley.
l) Ejercer las funciones de gestión, liquidación, inspección y recaudación en periodo voluntario de las aportaciones a realizar por los operadores de telecomunicaciones y por los prestadores privados del servicio de comunicación audiovisual televisiva, de ámbito geográfico estatal o superior al de una Comunidad Autónoma, reguladas en los artículos 5 y 6 de la Ley 8/2009, de 28 de agosto, de financiación de la Corporación Radio y Televisión Española.
m) Realizar las funciones atribuidas de manera expresa por la normativa comunitaria, la presente Ley y su normativa de desarrollo.
n) Realizar cualesquiera otras funciones que le sean atribuidas por ley o por real decreto.

Artículo 70. *La Comisión Nacional de los Mercados y la Competencia.*

1. La naturaleza, funciones, estructura, personal, presupuesto y demás materias que configuran la Comisión Nacional de los Mercados y la Competencia están reguladas en la Ley de creación de la Comisión Nacional de los Mercados y la Competencia.
2. En particular, en las materias reguladas por la presente Ley, la Comisión Nacional de los Mercados y la Competencia ejercerá las siguientes funciones:

a) Definir y analizar los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas, entre los que se incluirán los correspondientes mercados de referencia al por mayor y al por menor, y el ámbito geográfico de los mismos, cuyas características pueden justificar la imposición de obligaciones específicas, en los términos establecidos en el artículo 13 de la presente Ley y su normativa de desarrollo.
b) Identificar el operador u operadores que poseen un poder significativo en el mercado cuando del análisis de los mercados de referencia se constate que no se desarrollan en un entorno de competencia efectiva.
c) Establecer, cuando proceda, las obligaciones específicas que correspondan a los operadores con poder significativo en mercados de referencia, en los términos establecidos en el artículo 14 de la presente Ley y su normativa de desarrollo.

d) Resolver los conflictos en los mercados de comunicaciones electrónicas a los que se refiere el artículo 15 de la presente Ley.

En particular, le corresponderá resolver conflictos entre operadores relativos a la determinación de las condiciones concretas para la puesta en práctica de la obligación impuesta por el Ministerio de Industria, Energía y Turismo de la utilización compartida del dominio público o la propiedad privada, o de la ubicación compartida de infraestructuras y recursos asociados, de acuerdo con el procedimiento regulado en el artículo 32 de la presente Ley, así como resolver conflictos sobre el acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas y el acceso a las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal, en los términos establecidos por los artículos 37 y 38 de la presente Ley.

e) Decidir la imposición, como medida excepcional, a los operadores con poder significativo en el mercado integrados verticalmente, de la obligación de separación funcional de acuerdo con los requisitos y procedimientos indicados en el artículo 16 de la presente Ley.

f) Fijar las características y condiciones para la conservación de los números en aplicación de los aspectos técnicos y administrativos que mediante real decreto se establezcan para que ésta se lleve a cabo.

g) Intervenir en las relaciones entre operadores o entre operadores y otras entidades que se beneficien de las obligaciones de acceso e interconexión, con objeto de fomentar y, en su caso, garantizar la adecuación del acceso, la interconexión y la interoperabilidad de los servicios, en los términos establecidos en el artículo 12 de la presente Ley y su normativa de desarrollo.

h) Determinar la cuantía que supone el coste neto en la prestación del servicio universal, a que se refiere al artículo 27 de la presente Ley.

i) Definir y revisar la metodología para determinar el coste neto del servicio universal, tanto en lo que respecta a la imputación de costes como a la atribución de ingresos, que deberá basarse en procedimientos y criterios objetivos, transparentes, no discriminatorios y proporcionales y tener carácter público.

j) Establecer el procedimiento para cuantificar los beneficios no monetarios obtenidos por el operador u operadores encargados de la prestación del servicio universal.

k) Decidir la imposición de obligaciones a los operadores que dispongan de interfaces de programa de aplicaciones (API) y guías electrónicas de programación (EPG) para que faciliten el acceso a estos recursos, en la medida que sea necesario para garantizar el acceso de los usuarios finales a determinados servicios digitales de radiodifusión y televisión.

l) Ser consultada por el Gobierno y el Ministerio de Industria, Energía y Turismo en materia de comunicaciones electrónicas, particularmente en aquellas materias que puedan afectar al desarrollo libre y competitivo del mercado. Igualmente podrá ser consultada en materia de comunicaciones electrónicas por las comunidades autónomas y las corporaciones locales.

En el ejercicio de esta función, participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en materia de comunicaciones electrónicas.

m) Realizar las funciones de arbitraje, tanto de derecho como de equidad, que le sean sometidas por los operadores de comunicaciones electrónicas en aplicación de la Ley 60/2003, de 23 de diciembre, de Arbitraje.

n) Realizar las funciones atribuidas de manera expresa por la normativa comunitaria, la presente Ley y su normativa de desarrollo.

ñ) Realizar cualesquiera otras funciones que le sean atribuidas por ley o por real decreto.

TÍTULO VII

Tasas en materia de telecomunicaciones

Artículo 71. *Tasas en materia de telecomunicaciones.*

1. Las tasas en materia de telecomunicaciones gestionadas por la Administración General del Estado serán las recogidas en el anexo I de esta Ley.

2. Dichas tasas tendrán como finalidad:

a) Cubrir los gastos administrativos que ocasione el trabajo de regulación relativo a la preparación y puesta en práctica del derecho comunitario derivado y actos administrativos, como las relativas a la interconexión y acceso.

b) Los que ocasionen la gestión, control y ejecución del régimen establecido en esta Ley.

c) Los que ocasionen la gestión, control y ejecución de los derechos de ocupación del dominio público, los derechos de uso del dominio público radioeléctrico y la numeración.

d) La gestión de las notificaciones reguladas en el artículo 6 de esta Ley.

e) Los gastos de cooperación internacional, armonización y normalización y el análisis de mercado.

3. Sin perjuicio de lo dispuesto en el apartado 2, las tasas establecidas por el uso del dominio público radioeléctrico, la numeración y el dominio público necesario para la instalación de redes de comunicaciones electrónicas tendrán como finalidad la necesidad de garantizar el uso óptimo de estos recursos, teniendo en cuenta el valor del bien cuyo uso se otorga y su escasez. Dichas tasas deberán ser no discriminatorias, transparentes, justificadas objetivamente y ser proporcionadas a su fin. Asimismo, deberán fomentar el cumplimiento de los objetivos y principios establecidos en el artículo 3, en los términos que se establezcan mediante real decreto.

4. Las tasas a que se refieren los apartados anteriores serán impuestas de manera objetiva, transparente y proporcional, de manera que se minimicen los costes administrativos adicionales y las cargas que se derivan de ellos.

5. La revisión en vía administrativa de los actos de aplicación, gestión y recaudación de las tasas en materia de telecomunicaciones habrá de sujetarse a lo previsto en el artículo 22.3 de la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

6. El Ministerio de Industria, Energía y Turismo, respecto de las tasas a las que se refiere el apartado 1, y las administraciones competentes que gestionen y liquiden tasas subsumibles en el apartado 2 de este artículo, publicarán un resumen anual de los gastos administrativos que justifican su imposición y del importe total de la recaudación. Asimismo, las administraciones competentes que gestionen y liquiden tasas subsumibles en el apartado 3 de este artículo publicarán anualmente el importe total de la recaudación obtenida de los operadores de redes y servicios de comunicaciones electrónicas.

TÍTULO VIII

Inspección y régimen sancionador

Artículo 72. *Funciones inspectoras.*

1. La función inspectora en materia de telecomunicaciones corresponde a:

a) El Ministerio de Industria, Energía y Turismo.

b) La Comisión Nacional de los Mercados y la Competencia.

2. Será competencia del Ministerio de Industria, Energía y Turismo la inspección:

a) De los servicios y de las redes de comunicaciones electrónicas y de sus condiciones de prestación y explotación.

b) De los equipos y aparatos, de las instalaciones y de los sistemas civiles.

c) Del dominio público radioeléctrico.

d) De los servicios de tarificación adicional que se soporten sobre redes y servicios de comunicaciones electrónicas.

3. Corresponderá a la Comisión Nacional de los Mercados y la Competencia, en los términos establecidos en la Ley de creación de la Comisión Nacional de los Mercados y la Competencia, la inspección de las actividades de los operadores de telecomunicaciones respecto de las cuales tenga competencia sancionadora de conformidad con esta Ley.

4. Para la realización de determinadas actividades de inspección técnica, la Comisión Nacional de los Mercados y la Competencia, en materias de su competencia en el ámbito de aplicación de esta Ley, podrá solicitar la actuación del Ministerio de Industria, Energía y Turismo.

Artículo 73. *Facultades de inspección.*

1. Los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo tienen, en el ejercicio de sus funciones inspectoras en materia de telecomunicaciones, la consideración de autoridad pública y podrán solicitar, a través de la autoridad gubernativa correspondiente, el apoyo necesario de los Cuerpos y Fuerzas de Seguridad.

2. Los operadores o quienes realicen las actividades a las que se refiere esta Ley vendrán obligados a facilitar al personal de inspección, en el ejercicio de sus funciones, el acceso a sus instalaciones. También deberán permitir que dicho personal lleve a cabo el control de los elementos afectos a los servicios o actividades que realicen, de las redes que instalen o exploten y de cuantos documentos están obligados a poseer o conservar.

Los titulares de fincas o bienes inmuebles en los que se ubiquen equipos, estaciones o cualquier clase de instalaciones de telecomunicaciones tendrán la obligación de permitir el acceso a dichos bienes por parte del personal de Inspección a que se refiere este artículo. A estos efectos, el acceso por el personal de Inspección a las mencionadas fincas o inmuebles requerirá el consentimiento de dichos titulares o autorización judicial sólo cuando sea necesario entrar en un domicilio constitucionalmente protegido o efectuar registros en el mismo. Los órganos jurisdiccionales de lo Contencioso-Administrativo resolverán sobre el otorgamiento de la autorización judicial en el plazo máximo de 72 horas.

3. Los operadores o quienes realicen las actividades a las que se refiere esta Ley quedan obligados a poner a disposición del personal de inspección cuantos libros, registros y documentos, sea cual fuere su soporte, y medios técnicos éste considere precisos, incluidos los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase.

Asimismo, deberán facilitarles, a su petición, cualquier tipo de documentación que el personal de la Inspección les exija para la determinación de la titularidad de los equipos o la autoría de emisiones o actividades.

4. Las obligaciones establecidas en los dos apartados anteriores serán exigibles a los operadores o quienes realicen las actividades a las que se refiere esta Ley y que sean directamente responsables de la explotación de la red, la prestación del servicio o la realización de la actividad regulada por esta Ley, y también serán exigibles a quienes den soporte a las actuaciones anteriores, a los titulares de las fincas o los inmuebles en donde se ubiquen equipos o instalaciones de telecomunicaciones, a las asociaciones de empresas y a los administradores y otros miembros del personal de todas ellas.

5. Los operadores o quienes realicen las actividades a las que se refiere esta Ley están obligados a someterse a las inspecciones de los funcionarios del Ministerio de Industria, Energía y Turismo. La negativa u obstrucción al acceso a las instalaciones fincas o bienes inmuebles o a facilitar la información o documentación requerida será sancionada, conforme a los artículos siguientes de este título, como obstrucción a la labor inspectora.

6. En particular, el personal de inspección tendrá las siguientes facultades:

a) Precintar todos los locales, instalaciones, equipos, libros o documentos y demás bienes de la empresa durante el tiempo y en la medida en que sea necesario para la inspección.

b) Realizar comprobaciones, mediciones, obtener fotografías, vídeos, y grabaciones de imagen o sonido.

7. Las actuaciones de inspección, comprobación o investigación llevadas a cabo por el Ministerio de Industria, Energía y Turismo podrán desarrollarse, a elección de sus servicios:

a) En cualquier despacho, oficina o dependencia de la persona o entidad inspeccionada o de quien las represente.

b) En los propios locales del Ministerio de Industria, Energía y Turismo.

c) En cualquier despacho, oficina, dependencia o lugar en los que existan pruebas de los hechos objeto de inspección.

8. El personal de la Inspección del Ministerio de Industria, Energía y Turismo, a los efectos del cumplimiento de las funciones previstas en este artículo, tendrá acceso gratuito a todo registro público, en particular, en los Registros de la Propiedad y Mercantiles el acceso a la información registral se realizará por medios electrónicos, en la forma determinada en su normativa reguladora.

Artículo 74. *Responsabilidad por las infracciones en materia de telecomunicaciones.*

La responsabilidad administrativa por las infracciones de las normas reguladoras de las telecomunicaciones será exigible:

a) En el caso de incumplimiento de las condiciones establecidas para la explotación de redes o la prestación de servicios de comunicaciones electrónicas, a la persona física o jurídica que desarrolle la actividad.

b) En las cometidas con motivo de la explotación de redes o la prestación de servicios sin haber efectuado la notificación a que se refiere el artículo 6 de esta Ley o sin disponer de título habilitante para el uso del dominio público radioeléctrico cuando dicho título sea necesario, a la persona física o jurídica que realice la actividad.

Para identificar a la persona física o jurídica que realiza la actividad, se puede solicitar colaboración a la persona física o jurídica que tenga la disponibilidad de los equipos e instalaciones por cualquier título jurídico válido en derecho o careciendo de éste o a la persona física o jurídica titular de la finca o inmueble en donde se ubican los equipos e instalaciones. Si no se presta la citada colaboración de manera que dicha persona física o jurídica participa de manera esencial en la conducta infractora, se considerará que la misma es responsable de las infracciones cometidas por quien realiza la actividad. Esta responsabilidad es solidaria de la exigible a la persona física o jurídica que realiza la actividad.

c) En las cometidas por los usuarios, por las empresas instaladoras de telecomunicación, por los agentes económicos relacionados con equipos y aparatos de telecomunicación o por otras personas que, sin estar comprendidas en los párrafos anteriores, realicen actividades reguladas en la normativa sobre telecomunicaciones, a la persona física o jurídica cuya actuación se halle tipificada por el precepto infringido o a la que las normas correspondientes atribuyen específicamente la responsabilidad.

Artículo 75. *Clasificación de las infracciones.*

Las infracciones de las normas reguladoras de las telecomunicaciones se clasifican en muy graves, graves y leves.

Artículo 76. *Infracciones muy graves.*

Se consideran infracciones muy graves:

1. La realización de actividades sin disponer de la habilitación oportuna en las materias reguladas por esta Ley, cuando legalmente sea necesaria.

2. El incumplimiento de los requisitos exigibles para la explotación de las redes y prestación de los servicios de comunicaciones electrónicas establecidos en los artículos 6.1 y 6.2.

3. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos sin disponer de la concesión de uso privativo del dominio público radioeléctrico a que se refiere el artículo 62, cuando legalmente sea necesario.

4. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos no adecuada al correspondiente plan de utilización del espectro radioeléctrico o al Cuadro Nacional de Atribución de Frecuencias.

5. La realización de emisiones radioeléctricas no autorizadas que vulneren o perjudiquen el desarrollo o implantación de lo establecido en los Planes de utilización del dominio público radioeléctrico o en el Cuadro Nacional de Atribución de Frecuencias.

6. La producción deliberada, en España o en los países vecinos, de interferencias definidas como perjudiciales en esta Ley, incluidas las causadas por estaciones radioeléctricas que estén instaladas o en funcionamiento a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado que transmita emisiones desde fuera del territorio español para su posible recepción total o parcial en éste.

7. No atender el requerimiento de cesación hecho por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, en los supuestos de producción de interferencias.

8. La instalación, puesta en servicio o utilización de terminales o de equipos de telecomunicación, tanto los que hacen uso del dominio público radioeléctrico como los conectados, directa o indirectamente, a las redes públicas de comunicaciones electrónicas que no hayan evaluado su conformidad, conforme al Título IV de esta Ley, si se producen daños muy graves a las comunicaciones o a las redes.

9. La importación o la venta al por mayor de equipos o aparatos cuya conformidad no haya sido evaluada de acuerdo con lo dispuesto en el Título IV de esta Ley, o con los acuerdos o convenios internacionales celebrados por el Estado español.

10. La interceptación, sin autorización, de telecomunicaciones no destinadas al público en general, así como la divulgación del contenido.

11. El incumplimiento de las resoluciones firmes en vía administrativa o de las medidas previas y medidas cautelares a que se refieren los artículos 81 y 82 de esta Ley dictadas por el Ministerio de Industria, Energía y Turismo en el ejercicio de sus funciones en materia de comunicaciones electrónicas.

12. El incumplimiento de las resoluciones firmes en vía administrativa o de las medidas cautelares a que se refiere el artículo 82 de esta Ley dictadas por la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones en materia de comunicaciones electrónicas, con excepción de las que se lleve a cabo en el procedimiento arbitral previo sometimiento voluntario de las partes.

13. El incumplimiento de las resoluciones firmes en vía administrativa relativas a las reclamaciones por controversias entre los usuarios finales y los operadores.

14. La instalación negligente de infraestructuras comunes de telecomunicación en el interior de edificios y conjuntos inmobiliarios que sean causa de daños muy graves en las redes públicas de comunicaciones electrónicas.

15. El incumplimiento grave por parte de los operadores de las obligaciones en materia de acceso, interconexión e interoperabilidad de los servicios a las que estén sometidas por la vigente legislación.

16. El incumplimiento grave de las características y condiciones establecidas para la conservación de los números.

17. El incumplimiento reiterado mediante infracciones tipificadas como graves en los términos expresados en el artículo 79.4 de esta Ley.

Artículo 77. *Infracciones graves.*

Se consideran infracciones graves:

1. La instalación de estaciones radioeléctricas sin autorización, cuando, de acuerdo con lo dispuesto en la normativa reguladora de las telecomunicaciones, sea necesaria, o la instalación de estaciones radioeléctricas con características distintas a las autorizadas o, en su caso, a las contenidas en el proyecto técnico aprobado, o de estaciones radioeléctricas a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado, que, en el mar o fuera de él, posibilite la transmisión de emisiones desde el exterior para su posible recepción total o parcial en territorio nacional.

2. El uso del dominio público radioeléctrico en condiciones distintas a las previstas en el título habilitante oportuno a que se refiere el artículo 62, o, en su caso, distintas de las aprobadas en el proyecto técnico de las instalaciones, entre ellas utilizando parámetros técnicos distintos de los propios del título, o emplazamientos diferentes de los aprobados o potencias de emisión superiores a las autorizadas, cuando provoque alteraciones que dificulten la correcta prestación de otros servicios por otros operadores, en España o en los países vecinos.

3. El incumplimiento por los titulares de concesiones de uso privativo del dominio público radioeléctrico de las condiciones esenciales que se les impongan por el Ministerio de Industria, Energía y Turismo.

4. La mera producción, en España o en los países vecinos, de interferencias definidas como perjudiciales en esta Ley que no se encuentren comprendidas en el artículo anterior.

5. La emisión de señales de identificación falsas o engañosas.

6. Efectuar emisiones radioeléctricas que incumplan los límites de exposición establecidos en la normativa de desarrollo del artículo 61 de esta Ley e incumplir las demás medidas de seguridad establecidas en ella, incluidas las obligaciones de señalización o vallado de las instalaciones radioeléctricas. Asimismo, contribuir, mediante emisiones no autorizadas, a que se incumplan gravemente dichos límites.

7. La transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico, sin cumplir con los requisitos establecidos a tal efecto por la normativa de desarrollo de esta Ley.

8. El incumplimiento de las obligaciones que se deriven de las designaciones o acreditaciones que realice la Administración de telecomunicaciones en materia de evaluación de la conformidad de equipos y aparatos de telecomunicación, de conformidad con la normativa europea y nacional que les sean de aplicación.

9. La instalación, puesta en servicio o utilización de terminales o de equipos conectados a las redes públicas de comunicaciones electrónicas que no hayan evaluado su conformidad, conforme al Título IV de esta Ley.

10. La venta u oferta de venta, ya sea en establecimientos o por medios telemáticos o telefónicos, de equipos o aparatos cuya conformidad con los requisitos esenciales aplicables no haya sido evaluada de acuerdo con lo dispuesto en el Título IV de esta Ley o con las disposiciones, los acuerdos o convenios internacionales que obliguen al Estado español.

11. La negativa o la obstrucción a ser inspeccionado, la no colaboración con la inspección cuando ésta sea requerida y la no identificación por la persona física o jurídica que tenga la disponibilidad de los equipos e instalaciones o sea titular de la finca o inmueble en donde se ubican los equipos e instalaciones de la persona física o jurídica que explote redes o preste servicios sin haber efectuado la notificación a que se refiere el artículo 6 de esta Ley o sin disponer de título habilitante para el uso del dominio público radioeléctrico cuando dicho título sea necesario.

12. El ejercicio de la actividad de instalación y mantenimiento de equipos y sistemas de telecomunicación sin haber efectuado la declaración responsable o sin cumplir los requisitos a los que se refiere el artículo 59.

13. La instalación negligente de infraestructuras comunes de telecomunicación en el interior de edificios y conjuntos inmobiliarios que sean causa de daños en las redes públicas de comunicaciones electrónicas, salvo que deba ser considerada como infracción muy grave.

14. La alteración, la manipulación o la omisión del marcado de los equipos de telecomunicación en cualquiera de las partes donde reglamentariamente deban ser colocados; la alteración de la documentación de los equipos o de los manuales de instalación; así como el suministro de información para la alteración de las características técnicas o de las frecuencias de funcionamiento del aparato.

15. El incumplimiento por las entidades colaboradoras de la Administración para la normalización y la homologación de las prescripciones técnicas y del contenido de las autorizaciones o de los conciertos que les afecten, con arreglo a lo que reglamentariamente se determine.

16. La negativa a cumplir las obligaciones de servicio público según lo establecido en el Título III de la Ley y su normativa de desarrollo.

17. La negativa a cumplir las condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas.

18. El cumplimiento tardío o defectuoso por los operadores de las resoluciones firmes en vía administrativa relativas a las reclamaciones por controversias entre los usuarios finales y los operadores.

19. El incumplimiento de las condiciones determinantes de las atribuciones y el otorgamiento de los derechos de uso de los recursos de numeración incluidos en los planes de numeración.

20. El incumplimiento por los operadores de las obligaciones relativas a la integridad y seguridad en la prestación de servicios o la explotación de redes de comunicaciones electrónica.

21. El incumplimiento por los operadores de las obligaciones establecidas para la utilización compartida del dominio público o la propiedad privada en que se van a establecer las redes públicas de comunicaciones electrónicas o el uso compartido de las infraestructuras y recursos asociados.

22. El incumplimiento por los operadores, o por los propietarios de los correspondientes recursos asociados, de las obligaciones establecidas para la utilización compartida de los tramos finales de las redes de acceso.

23. El incumplimiento de las obligaciones relacionadas con la utilización de normas o especificaciones técnicas declaradas obligatorias por la Comisión Europea.

24. La alteración, la manipulación o la omisión de las características técnicas en la documentación de las instalaciones comunes de telecomunicación en el interior de edificios y conjuntos inmobiliarios que se presente a la Administración o a los propietarios.

25. El incumplimiento por los operadores controlados directa o indirectamente por administraciones públicas de las obligaciones establecidas en el artículo 9.

26. El cumplimiento tardío o defectuoso de las resoluciones firmes en vía administrativa o de las medidas previas y medidas cautelares a que se refieren los artículos 81 y 82 de esta Ley dictadas por el Ministerio de Industria, Energía y Turismo en el ejercicio de sus funciones en materia de comunicaciones electrónicas.

27. El cumplimiento tardío o defectuoso de las resoluciones firmes en vía administrativa o de las medidas cautelares a que se refiere el artículo 82 de esta Ley dictadas por la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones en materia de comunicaciones electrónicas, con excepción de las que se lleve a cabo en el procedimiento arbitral previo sometimiento voluntario de las partes.

28. El incumplimiento por parte de los operadores de las obligaciones en materia de acceso, interconexión e interoperabilidad de los servicios a las que estén sometidas por la vigente legislación.

29. La falta de notificación a la Administración por el titular de una red de comunicaciones electrónicas de los servicios que se estén prestando a través de ella cuando esta información sea exigible de acuerdo con la normativa aplicable.

30. La puesta a disposición de redes públicas de comunicaciones electrónicas a favor de entidades para que se realicen emisiones radioeléctricas cuando no se ostente el correspondiente título habilitante para el uso del dominio público radioeléctrico.

31. La expedición de certificaciones de instalaciones de telecomunicación que no concuerden con la realidad.

32. El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 39 de la presente Ley.

33. Cursar tráfico contrario a planes nacionales e internacionales de numeración.

34. Cursar tráfico irregular con fines fraudulentos en las redes públicas y servicios de comunicaciones electrónicas disponibles al público.

35. No facilitar, cuando resulte exigible conforme a lo previsto por la normativa reguladora de las comunicaciones electrónicas, los datos requeridos por la Administración una vez transcurridos tres meses a contar desde la finalización del plazo otorgado en el requerimiento de información o una vez finalizado el plazo otorgado en el segundo requerimiento de la misma información.

36. El incumplimiento de las características y condiciones establecidas para la conservación de los números.

37. La vulneración grave de los derechos de los consumidores y usuarios finales, según lo establecido en el título III de la Ley y su normativa de desarrollo.

38. El incumplimiento reiterado mediante infracciones tipificadas como leves en los términos expresados en el artículo 79.4 de esta Ley.

Artículo 78. *Infracciones leves.*

Se consideran infracciones leves:

1. La producción de cualquier tipo de emisión radioeléctrica no autorizada o no adecuada con el correspondiente plan de utilización del espectro radioeléctrico, salvo que deba ser considerada como infracción grave o muy grave.

2. El establecimiento de comunicaciones utilizando estaciones no autorizadas.

3. La mera producción de interferencias, en España o en los países vecinos, cuando no deba ser considerada como infracción grave o muy grave.

4. No facilitar los datos requeridos por la Administración o retrasar injustificadamente su aportación cuando resulte exigible conforme a lo previsto por la normativa reguladora de las comunicaciones electrónicas.

5. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos sin disponer de la autorización general, autorización individual o afectación demanial para el uso del dominio público radioeléctrico a las que se refiere el artículo 62, cuando legalmente sea necesario.

6. La instalación de estaciones radioeléctricas de radioaficionado careciendo de autorización.

7. El incumplimiento por los titulares de autorizaciones generales, autorizaciones individuales o afectaciones demaniales para el uso del dominio público radioeléctrico de las condiciones esenciales que se les impongan por el Ministerio de Industria, Energía y Turismo.

8. La explotación de redes o la prestación de servicios de comunicaciones electrónicas sin cumplir los requisitos exigibles para realizar tales actividades establecidos en esta Ley y su normativa de desarrollo distintos de los previstos en los artículos 6.1 y 6.2.

9. La instalación de infraestructuras de telecomunicaciones sin cumplir los requisitos establecidos en la presente Ley, salvo que deba ser considerada como infracción grave o muy grave.

10. El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 39 de la presente Ley, cuando no se califique como infracción muy grave o grave.

11. El incumplimiento de las obligaciones de servicio público, de las obligaciones de carácter público y la vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el Título III de la Ley y su normativa de desarrollo.

12. El incumplimiento de las obligaciones en materia de calidad de servicio.

13. La no presentación de la documentación de las instalaciones comunes de telecomunicaciones a la administración o a la propiedad, cuando normativamente sea obligatoria dicha presentación.

Artículo 79. *Sanciones.*

1. Por la comisión de las infracciones tipificadas en los artículos anteriores se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves se impondrá al infractor multa por importe de hasta veinte millones de euros.

Por la comisión de infracciones muy graves tipificadas en las que la Comisión Nacional de los Mercados y la Competencia tenga competencias sancionadoras se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción será de 20 millones de euros.

b) Las infracciones muy graves, en función de sus circunstancias, podrán dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas. También podrá dar lugar a la inhabilitación hasta cinco años para el ejercicio de la actividad de instalador.

c) Por la comisión de infracciones graves se impondrá al infractor multa por importe de hasta dos millones de euros.

Por la comisión de infracciones graves tipificadas en las que la Comisión Nacional de los Mercados y la Competencia tenga competencias sancionadoras se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio, el límite máximo de la sanción será de dos millones de euros.

d) Por la comisión de infracciones leves se impondrá al infractor una multa por importe de hasta 50.000 euros.

2. Las sanciones impuestas por cualquiera de las infracciones comprendidas en los artículos 76 y 77, cuando se requiera título habilitante para el ejercicio de la actividad realizada por el infractor, podrán llevar aparejada, como sanción accesoria, el precintado o la incautación de los equipos o aparatos o la clausura de las instalaciones en tanto no se disponga del referido título.

3. Además de la sanción que corresponda imponer a los infractores, cuando se trate de una persona jurídica, se podrá imponer una multa de hasta 5.000 euros en el caso de las infracciones leves, hasta 30.000 euros en el caso de las infracciones graves y hasta 60.000 euros en el caso de las infracciones muy graves a sus representantes legales o a las personas que integran los órganos directivos que hayan intervenido en el acuerdo o decisión.

Quedan excluidas de la sanción aquellas personas que, formando parte de órganos colegiados de administración, no hubieran asistido a las reuniones o hubieran votado en contra o salvando su voto.

4. A los efectos de lo establecido en esta Ley, tendrá la consideración de incumplimiento reiterado la sanción definitiva de dos o más infracciones del mismo tipo infractor en el período de tres años.

Artículo 80. *Criterios para la determinación de la cuantía de la sanción.*

1. La cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común, lo siguiente:

a) La gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona.

b) La repercusión social de las infracciones.

c) El beneficio que haya reportado al infractor el hecho objeto de la infracción.

d) El daño causado y su reparación.

e) El cumplimiento voluntario de las medidas cautelares que, en su caso, se impongan en el procedimiento sancionador.

f) La negativa u obstrucción al acceso a las instalaciones o a facilitar la información o documentación requerida.

g) El cese de la actividad infractora, previamente o durante la tramitación del expediente sancionador.

2. Para la fijación de la sanción también se tendrá en cuenta la situación económica del infractor, derivada de su patrimonio, de sus ingresos, de sus posibles cargas familiares y de las demás circunstancias personales que acredite que le afectan.

El infractor vendrá obligado, en su caso, al pago de las tasas que hubiera debido satisfacer en el supuesto de haber realizado la notificación a que se refiere el artículo 6 o de haber disfrutado de título para la utilización del dominio público radioeléctrico.

Artículo 81. *Medidas previas al procedimiento sancionador.*

1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Industria, Energía y Turismo, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) Cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de Seguridad Pública, Protección Civil y de Emergencias.
b) Cuando la realización de la presunta actividad infractora pueda poner en peligro la vida humana.
c) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

2. Esta orden de cese irá dirigida a cualquier sujeto que se encuentre en disposición de ejecutar tal cese, sin perjuicio de la posterior delimitación de responsabilidades en el correspondiente procedimiento sancionador. Para su ejecución forzosa, la resolución podrá disponer que, a través de la Autoridad Gubernativa, se facilite apoyo por los Cuerpos y Fuerzas de Seguridad.
En la resolución se determinará el ámbito objetivo y temporal de la medida, sin que pueda exceder del plazo de un mes.

Artículo 82. *Medidas cautelares en el procedimiento sancionador.*

1. Las infracciones a las que se refieren los artículos 76 y 77 podrán dar lugar, una vez incoado el expediente sancionador, a la adopción de medidas cautelares que, de conformidad con el artículo 136 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y del Procedimiento Administrativo Común, podrán consistir en las siguientes:

a) Ordenar el cese inmediato de emisiones radioeléctricas no autorizadas.
b) Orden de cese inmediato de cualquier otra actividad presuntamente infractora.

Entre ellas,

i) Emitir órdenes de poner fin a la prestación de un servicio o de una serie de servicios, o aplazarla cuando dicha prestación pudiera tener como resultado perjudicar seriamente la competencia, hasta que se cumplan las obligaciones específicas impuestas a raíz de un análisis de mercado con arreglo al artículo 14. Esta medida, junto con las razones en que se basa, se comunicará al operador afectado sin demora, fijando un plazo razonable para que la empresa cumpla con la misma.
ii) Impedir que un operador siga suministrando redes o servicios de comunicaciones electrónicas o suspender o retirarle sus derechos de uso, en caso de incumplimiento grave y reiterado de las condiciones establecidas para la prestación de servicios o la explotación de redes o para el otorgamiento de derechos de uso o de las obligaciones específicas que se hubieran impuesto, cuando hubieran fracasado las medidas destinadas a exigir el cese de la infracción.
iii) Adoptar medidas provisionales de urgencia destinadas a remediar incumplimientos de las condiciones establecidas para la prestación de servicios o la explotación de redes o para el otorgamiento de derechos de uso o de las obligaciones específicas que se hubieran impuesto, cuando los mismos representen una amenaza inmediata y grave para la seguridad pública o la salud pública o creen graves problemas económicos u operativos a otros suministradores o usuarios del espectro radioeléctrico. Posteriormente deberá ofrecerse al operador interesado la posibilidad de proponer posibles soluciones. En su caso, la autoridad competente podrá confirmar las medidas provisionales, que podrán mantenerse hasta la resolución que ponga fin al procedimiento sancionador.

c) El precintado de los equipos o instalaciones que hubiera empleado el infractor, siendo, en su caso, aplicable el régimen de ejecución subsidiaria previsto en el artículo 98 de dicha Ley.

d) La retirada del mercado de los equipos y aparatos que presuntamente no hayan evaluado su conformidad de acuerdo con la normativa aplicable.

e) La suspensión provisional de la eficacia del título y la clausura provisional de las instalaciones, por un plazo máximo de seis meses.

2. Cuando el infractor carezca de título habilitante para la ocupación o uso del dominio público radioeléctrico, o si con la infracción se superan los niveles de emisiones radioeléctricas establecidos en la normativa de desarrollo del artículo 61, la medida cautelar prevista en el párrafo a) del apartado anterior será obligatoriamente incluida en el acuerdo de iniciación de expediente sancionador, con objeto de salvaguardar el correcto uso de dicho dominio público.

3. Sin perjuicio de los supuestos en los que este precepto fija un plazo máximo de duración, las medidas cautelares podrán mantenerse hasta la resolución del procedimiento sancionador, siempre que se considere necesario para asegurar la eficacia de la resolución final que pudiera recaer. Como excepción, la medida cautelar de retirada del mercado de los equipos y aparatos cuya conformidad no haya sido evaluada presuntamente de acuerdo con la normativa aplicable deberá levantarse cuando se acredite la realización de la evaluación de la conformidad de los equipos y aparatos afectados.

Artículo 83. *Prescripción.*

1. Las infracciones reguladas en esta Ley prescribirán, las muy graves, a los tres años; las graves, a los dos años, y las leves, al año.

El plazo de prescripción de las infracciones comenzará a computarse desde el día en que se hubieran cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador. El plazo de prescripción volverá a correr si el expediente sancionador estuviera paralizado durante más de un mes por causa no imputable al presunto responsable.

En el supuesto de infracción continuada, la fecha inicial del cómputo será aquella en que deje de realizarse la actividad infractora o la del último acto con que la infracción se consume. No obstante, se entenderá que persiste la infracción en tanto los equipos, aparatos o instalaciones objeto del expediente no se encuentren a disposición de la Administración o quede constancia fehaciente de su imposibilidad de uso.

2. Las sanciones impuestas por faltas muy graves prescribirán a los tres años; las impuestas por faltas graves, a los dos años, y las impuestas por faltas leves, al año. El plazo de prescripción de las sanciones comenzará a computarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a correr el plazo si aquél está paralizado durante más de un mes por causa no imputable al infractor.

Artículo 84. *Competencias sancionadoras.*

La competencia sancionadora corresponderá:

1. Al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, para la imposición de sanciones no contempladas en los siguientes apartados.

2. A la Comisión Nacional de los Mercados y la Competencia, en el ámbito material de su actuación, cuando se trate de infracciones muy graves tipificadas en los apartados 12, 15 y 16 del artículo 76, infracciones graves tipificadas en los apartados 11, 27, 28, 35 y 36 del artículo 77 e infracciones leves tipificadas en el apartado 4 del artículo 78.

3. A la Agencia Española de Protección de Datos, en el caso de que se trate de las infracciones graves del artículo 77 tipificadas en el apartado 37 y de las infracciones leves del artículo 78 tipificadas en el apartado 11 cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en el artículo 48.

4. El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las administraciones públicas. No obstante, el plazo máximo de duración del procedimiento será de un año y el plazo de alegaciones no tendrá una duración inferior a un mes.

Disposición adicional primera. *Significado de los términos empleados por esta Ley.*

A los efectos de esta Ley, los términos definidos en el anexo II tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Limitaciones y servidumbres.*

1. Las limitaciones a la propiedad y las servidumbres a las que hace referencia el apartado 1 del artículo 33 de esta Ley podrán afectar:

a) A la altura máxima de los edificios.
b) A la distancia mínima a la que podrán ubicarse industrias e instalaciones eléctricas de alta tensión y líneas férreas electrificadas.
c) A la distancia mínima a la que podrán instalarse transmisores radioeléctricos.

2. Con la excepción de la normativa legal vigente aplicable a la defensa nacional y a la navegación aérea, no podrán establecerse, por vía reglamentaria, limitaciones a la propiedad ni servidumbres que contengan condiciones más gravosas que las siguientes:

a) Para distancias inferiores a 1.000 metros, el ángulo sobre la horizontal con el que se observe, desde la parte superior de las antenas receptoras de menor altura de la estación, el punto más elevado de un edificio será como máximo de tres grados.
b) La máxima limitación exigible de separación entre una industria o una línea de tendido eléctrico de alta tensión o de ferrocarril y cualquiera de las antenas receptoras de la estación será de 1.000 metros.

La instalación de transmisores radioeléctricos en las proximidades de la estación se realizará con las siguientes limitaciones:

Gama de frecuencias	Potencia radiada aparente del transmisor en dirección a la instalación a proteger – Kilovatios	Máxima limitación exigible de separación entre instalaciones a proteger y antena del transmisor – Kilómetros
f ≤ 30 MHz	0,01 < P < 1	2
	1 < P ≤10	10
	P > 10	20
f > 30 MHz	0,01 < P ≤ 1	1
	1 < P ≤ 10	2
	P > 10	5

3. Las limitaciones de intensidad de campo eléctrico se exigirán para aquellas instalaciones cuyos equipos tengan una alta sensibilidad. Se entiende que utilizan equipos de alta sensibilidad las instalaciones dedicadas a la investigación:

a) Las estaciones dedicadas a la observación radioastronómica, estas limitaciones serán las siguientes:

Niveles máximos admisibles de densidad espectral de flujo de potencia en las estaciones de observación de Radioastronomía [(1) (2)]

Frecuencia central (MHz)	Anchura de banda de canal (kHz)	Densidad espectral de flujo de potencia (dB(W/(m² · Hz)))	Observaciones radioastronómicas
13,385	50	–248	Continuo.
25,61	120	–249	Continuo.
151,525	2950	–259	Continuo.
325,3	6600	–258	Continuo.
327	10	–244	Rayas espectrales.
408,05	3900	–255	Continuo.
1413,5	27000	–255	Continuo.
1420	20	–239	Rayas espectrales.
1612	20	–238	Rayas espectrales.

Frecuencia central (MHz)	Anchura de banda de canal (kHz)	Densidad espectral de flujo de potencia (dB(W/(m² · Hz)))	Observaciones radioastronómicas
1665	20	–237	Rayas espectrales.
1665	10000	–251	Continuo.
2695	10000	–247	Continuo.
4995	10000	–241	Continuo.
10650	100000	–240	Continuo.
15375	50000	–233	Continuo.
22200	250	–216	Rayas espectrales.
22355	290000	–231	Continuo.
23700	250	–215	Rayas espectrales.
23800	400000	–233	Continuo.
31550	500000	–228	Continuo.
43000	500	–210	Rayas espectrales.
43000	1000000	–227	Continuo.
76750	8000000	–229	Continuo.
82500	8000000	–228	Continuo.
88600	1000	–208	Rayas espectrales.
89000	8000000	–228	Continuo.
105050	8000000	–223	Continuo.
132000	8000000	–223	Continuo.
147250	8000000	–223	Continuo.
150000	1000	–204	Rayas espectrales.
165500	8000000	–222	Continuo.
183500	8000000	–220	Continuo.
215750	8000000	–218	Continuo.
220000	1000	–199	Rayas espectrales.
244500	8000000	–217	Continuo.
265000	1000	–197	Rayas espectrales.
270000	8000000	–216	Continuo.

(1) Los valores anteriores corresponden a una ganancia supuesta de la antena receptora de radioastronomía de 0 dBi.

(2) Para sistemas interferentes con condiciones de propagación variables en el tiempo los niveles dados no podrán ser excedidos en la medida en que la pérdida de datos supere el 2%.

b) Para la protección de las instalaciones de observatorios de astrofísica, la limitación de la intensidad de campo eléctrico, en cualquier frecuencia, será de 88,8 dB (μV/m) en la ubicación del observatorio.

4. Para un mejor aprovechamiento del espectro radioeléctrico, la Administración podrá imponer la utilización en las instalaciones de aquellos elementos técnicos que mejoren la compatibilidad radioeléctrica entre estaciones.

Disposición adicional tercera. *Aplicación de la legislación reguladora de las infraestructuras comunes en los edificios.*

Las infraestructuras comunes de telecomunicaciones en el interior de los edificios se regulan por lo establecido en la presente Ley, por el real decreto-Ley 1/1998, de 27 de febrero, sobre infraestructuras comunes en los edificios para el acceso a los servicios de telecomunicación y sus desarrollos reglamentarios.

Disposición adicional cuarta. *Información confidencial.*

Las personas físicas o jurídicas que aporten a alguna Autoridad Nacional de Reglamentación datos o informaciones de cualquier tipo, con ocasión del desempeño de sus funciones y respetando la legislación vigente en materia de protección de datos y privacidad, podrán indicar, de forma justificada, qué parte de lo aportado consideran confidencial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad. Cada Autoridad Nacional de Reglamentación decidirá, de forma motivada y a través de las resoluciones oportunas, sobre la información que, según la legislación vigente, resulte o no amparada por la confidencialidad.

Disposición adicional quinta. *El Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.*

1. El Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, presidido por el Ministro de Industria, Energía y Turismo o por la persona en quien delegue, es un órgano asesor del Gobierno en materia de telecomunicaciones y sociedad de la información.

2. Las funciones del Consejo serán de estudio, deliberación y propuesta en materias relativas a las telecomunicaciones y a la sociedad de la información, sin perjuicio de las competencias que correspondan a los órganos colegiados interministeriales con competencias de informe al Gobierno en materia de política informática. Le corresponderá, igualmente, informar sobre los asuntos que el Gobierno determine o sobre los que, por propia iniciativa, juzgue conveniente. La deliberación de proyectos o propuestas normativas en el seno del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información equivaldrá a la audiencia a la que se refiere el artículo 24.1.c) de la Ley 50/1997, de 27 de noviembre, del Gobierno.

El Gobierno, mediante real decreto, establecerá la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, cuyos miembros representarán a la Administración General del Estado, a las Administraciones autonómicas, a la Administración local a través de sus asociaciones o federaciones más representativas, a los usuarios, incluyendo en todo caso a las personas con discapacidad a través de su organización más representativa, a los operadores que presten servicios o exploten redes públicas de comunicaciones electrónicas, a los prestadores de servicios de comunicación audiovisual, a los prestadores de servicios de la sociedad de la información, a las industrias fabricantes de equipos de telecomunicaciones y de la sociedad de la información, a los sindicatos y a los colegios oficiales de ingeniería más representativos del sector.

Disposición adicional sexta. *Multas coercitivas.*

Para asegurar el cumplimiento de las resoluciones o requerimientos de información que dicten, el Ministerio de Industria, Energía y Turismo o la Comisión Nacional de los Mercados y de la Competencia podrán imponer multas coercitivas por importe diario de 125 hasta 30.000 euros, en los términos previstos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Las multas coercitivas serán independientes de las sanciones que puedan imponerse y compatibles con ellas.

El importe de las multas coercitivas previstas en esta disposición se ingresará en el Tesoro Público.

Disposición adicional séptima. *Obligaciones en materia de acceso condicional, acceso a determinados servicios de radiodifusión y televisión, televisión de formato ancho y obligaciones de transmisión.*

1. Mediante real decreto se podrán establecer las condiciones aplicables a los operadores de redes públicas de comunicaciones electrónicas en materia de acceso condicional a los servicios de televisión y radio digitales difundidos a los telespectadores y oyentes, con independencia del medio de transmisión utilizado. Asimismo, se regulará mediante real decreto el procedimiento de revisión de dichas condiciones por la Comisión Nacional de los Mercados y la Competencia, en el supuesto de que el operador obligado ya no tuviera poder significativo en el mercado en cuestión.

2. En la medida que sea necesario para garantizar el acceso de los usuarios finales a determinados servicios digitales de radiodifusión y televisión, la Comisión Nacional de los Mercados y la Competencia podrá imponer, en la forma y para los servicios que se determinen mediante real decreto por el Gobierno, obligaciones a los operadores que dispongan de interfaces de programa de aplicaciones (API) y guías electrónicas de programación (EPG) para que faciliten el acceso a estos recursos en condiciones razonables, justas y no discriminatorias.

3. Las redes públicas de comunicaciones electrónicas utilizadas para la distribución de servicios de televisión digital deberán disponer de capacidad para distribuir programas y servicios de televisión de formato ancho. Los operadores de dichas redes que reciban programas o servicios de televisión de formato ancho para su posterior distribución estarán obligados a mantener dicho formato.

4. Mediante real decreto aprobado por el Consejo de Ministros podrán imponerse, como obligaciones de servicio público, exigencias razonables de transmisión de determinados canales de programas de radio y televisión, así como exigencias de transmisión de servicios complementarios para posibilitar el acceso adecuado de los usuarios con discapacidad, a los operadores que exploten redes de comunicaciones electrónicas utilizadas para la distribución de programas de radio o televisión al público, si un número significativo de usuarios finales de dichas redes las utiliza como medio principal de recepción de programas de radio y televisión, cuando resulte necesario para alcanzar objetivos de interés general claramente definidos y de forma proporcionada, transparente y periódicamente revisable.

Asimismo, podrán establecerse mediante real decreto condiciones a los proveedores de servicios y equipos de televisión digital, para que cooperen en la prestación de servicios de comunicación audiovisual televisiva interoperables para los usuarios finales con discapacidad.

5. Mediante Orden ministerial se regulará el establecimiento de las obligaciones y requisitos para los gestores de múltiples digitales de la televisión digital terrestre y la creación y regulación del Registro de parámetros de información de los servicios de televisión digital terrestre. La gestión, asignación y control de los parámetros de información de los servicios de televisión digital terrestre y la llevanza de dicho Registro corresponde al Ministerio de Industria, Energía y Turismo.

Disposición adicional octava. *Mecanismo de notificación.*

Las medidas adoptadas por una autoridad nacional de reglamentación de acuerdo con los artículos 13, 14 y 16 y de la disposición adicional séptima de esta Ley y de su normativa de desarrollo, así como todas aquellas medidas que pudieran tener repercusiones en los intercambios entre Estados miembros, se someterán a los mecanismos de notificación a que se refieren artículos 7, 7 bis y 7 ter de la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y de los servicios de comunicaciones electrónicas (Directiva Marco) y las normas dictadas al efecto en desarrollo de las mismos por la Unión Europea.

Disposición adicional novena. *Informe sobre las obligaciones a imponer a operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público.*

Cualquier medida normativa que vaya a aprobarse con posterioridad a la entrada en vigor de la presente Ley o acto administrativo en ejecución de dicha medida normativa que tramite cualquier Administración Pública y que persiga imponer con carácter generalizado a los operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público o a un grupo específico de los mismos obligaciones de servicio público distintas de las previstas en el artículo 28 de esta Ley, obligaciones de supervisión de la información tratada o gestionada en dichas redes o servicios o de colaboración con los agentes facultados respecto al tráfico gestionado, requerirá el informe preceptivo del Ministerio de Industria, Energía y Turismo.

Dicha medida normativa o acto administrativo deberá contemplar de manera expresa los mecanismos de financiación de los costes derivados de las obligaciones de servicio público distintas de las previstas en el artículo 28 de esta Ley, obligaciones de carácter público o cualquier otra carga administrativa que se imponga, que no podrá ser a cargo de los operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público cuando se traten de obligaciones o cargas que no deriven directamente del marco normativo de las comunicaciones electrónicas sino que respondan a otras razones de políticas públicas, salvo que concurran motivos de interés público que lleven a la conclusión de que dichos operadores deban asumir dichos costes, aun cuando sea parcialmente.

La solicitud del preceptivo informe del Ministerio de Industria, Energía y Turismo se considera un requisito esencial en la tramitación de la norma o acto administrativo.

Disposición adicional décima. *Creación de la Comisión Interministerial sobre radiofrecuencias y salud.*

Mediante real decreto se regulará la composición, organización y funciones de la Comisión Interministerial sobre radiofrecuencias y salud, cuya misión es la de asesorar e informar a la ciudadanía, al conjunto de las administraciones públicas y a los diversos agentes de la industria sobre las restricciones establecidas a las emisiones radioeléctricas, las medidas de protección sanitaria aprobadas frente a emisiones radioeléctricas y los múltiples y periódicos controles a que son sometidas las instalaciones generadoras de emisiones radioeléctricas, en particular, las relativas a las radiocomunicaciones. Asimismo, dicha Comisión realizará y divulgará estudios e investigaciones sobre las emisiones radioeléctricas y sus efectos y cómo las restricciones a las emisiones, las medidas de protección sanitaria y los controles establecidos preservan la salud de las personas, así como, a la vista de dichos estudios e investigaciones, realizará propuestas y sugerirá líneas de mejora en las medidas y controles a realizar.

De la Comisión interministerial formarán parte en todo caso el Ministerio de Industria, Energía y Turismo, el Ministerio de Sanidad, Servicios Sociales e Igualdad, y el Instituto de Salud Carlos III por parte del Ministerio de Economía y Competitividad.

Dicha Comisión contará con un grupo asesor o colaborador en materia de radiofrecuencias y salud, con participación de Comunidades Autónomas, de la asociación de entidades locales de ámbito estatal con mayor implantación y un grupo de expertos independientes, sociedades científicas y representantes de los ciudadanos, para hacer evaluación y seguimiento periódico de la prevención y protección de la salud de la población en relación con las emisiones radioeléctricas, proponiendo estudios de investigación, medidas consensuadas de identificación, elaboración de registros y protocolos de atención al ciudadano.

La creación y el funcionamiento tanto de la Comisión como del Grupo asesor se atenderán con los medios personales, técnicos y presupuestarios actuales asignados a los Ministerios y demás Administraciones participantes, sin incremento en el gasto público.

Disposición adicional undécima. *Parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas.*

Los parámetros y requerimientos técnicos esenciales que son indispensables para garantizar el funcionamiento de las redes y servicios de comunicaciones electrónicas se establecerán mediante real decreto aprobado en Consejo de Ministros.

Disposición adicional duodécima. *Aplicación de la Ley General Tributaria.*

Lo previsto en la presente Ley, se entenderá sin perjuicio de las competencias y facultades que la Ley 58/2003, de 17 de diciembre, General Tributaria, atribuye a la Administración Tributaria, en particular, en relación con el acceso a los datos con trascendencia tributaria.

Disposición adicional decimotercera. *Publicación de actos.*

Los actos que formen parte de las distintas fases de los procedimientos que tramite el Ministerio de Industria, Energía y Turismo en el ejercicio de las competencias y funciones asignadas en las materias a que se refiere la presente Ley se podrán publicar en el «Boletín Oficial del Estado», de conformidad con lo previsto en el artículo 60 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común. Asimismo, todas aquellas resoluciones, actos administrativos o actos de trámite dictados por el Ministerio de Industria, Energía y Turismo en el ejercicio de las competencias y funciones asignadas en las materias a que se refiere la presente Ley y que pudieran tener un número indeterminado de potenciales interesados que requieran ser notificados, deberán ser publicados en el «Boletín Oficial del Estado», de conformidad con lo previsto en la letra a) del artículo 59.6 de la Ley 30/1992, de 26 de noviembre.

Disposición adicional decimocuarta. *Coordinación de las ayudas públicas a la banda ancha y al desarrollo de la economía y empleo digitales y nuevos servicios digitales.*

Por real decreto se identificarán los órganos competentes y se establecerán los procedimientos de coordinación entre Administraciones y Organismos públicos, en relación con las ayudas públicas a la banda ancha, cuya convocatoria y otorgamiento deberá respetar en todo caso el marco comunitario y los objetivos estipulados en el artículo 3 de la presente ley y en relación con el fomento de la I + D + I y a las actuaciones para el desarrollo de la economía, el empleo digital y todos los nuevos servicios digitales que las nuevas redes ultrarrápidas permiten, garantizando la cohesión social y territorial.

Disposición adicional decimoquinta. *Asignación de medios a la Administración General del Estado e integración de personal de la Comisión Nacional de los Mercados y la Competencia.*

1. El Gobierno aprobará las modificaciones necesarias en el real decreto de desarrollo de la estructura orgánica básica del Ministerio de Industria, Energía y Turismo para garantizar el ejercicio de las funciones que, siendo competencia de la Comisión Nacional de los Mercados y la Competencia hasta el momento de la entrada en vigor de la presente Ley, ésta atribuye al Ministerio de Industria, Energía y Turismo.

La entrada en vigor de la modificación del real decreto de estructura orgánica básica del Ministerio de Industria, Energía y Turismo no se producirá hasta que el presupuesto del Ministerio de Industria, Energía y Turismo no se adecue a la nueva distribución competencial y se haya llevado a cabo la asunción de medios materiales, incluyendo, en particular, sistemas y aplicaciones informáticas, y la integración de personal procedente de la Comisión Nacional de los Mercados y la Competencia que resulte necesario para que el Ministerio de Industria, Energía y Turismo pueda ejercer las nuevas funciones atribuidas.

2. El personal de la Comisión Nacional de los Mercados y la Competencia que viene ejerciendo las funciones que, siendo competencia de la citada Comisión hasta el momento de la entrada en vigor de la presente Ley, ésta atribuye al Ministerio de Industria, Energía y Turismo, se integrará en la Administración General del Estado en los términos indicados en la disposición adicional sexta de la Ley de creación de la Comisión Nacional de los Mercados y la Competencia.

3. La fecha para el ejercicio efectivo de las nuevas funciones que esta Ley atribuye al Ministerio de Industria, Energía y Turismo se determinará mediante orden del Ministro de la Presidencia, a propuesta del Ministro de Industria, Energía y Turismo, del Ministro de Economía y Competitividad y del Ministro de Hacienda y Administraciones públicas. En todo caso, todas las actuaciones a que se refiere la presente disposición deberán haberse realizado en el plazo de cuatro meses desde la entrada en vigor de esta Ley.

Disposición adicional decimosexta. *La entidad pública empresarial Red.es.*

1. La entidad Red.es, creada por la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, se configura como entidad pública empresarial, conforme a lo previsto en el artículo 43.1.b) de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Dicha entidad queda adscrita al Ministerio de Industria, Energía y Turismo, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

2. La entidad pública empresarial Red.es tiene personalidad jurídica propia, plena capacidad de obrar y patrimonio propio y se regirá por lo establecido en esta disposición adicional, en su propio Estatuto, en la citada Ley 6/1997 y en las demás normas que le sean de aplicación.

3. Constituye el objeto de la entidad pública empresarial la gestión, administración y disposición de los bienes y derechos que integran su patrimonio, correspondiéndole la tenencia, administración, adquisición y enajenación de los títulos representativos del capital de las sociedades en las que participe o pueda participar en el futuro. La entidad pública empresarial actuará, en cumplimiento de su objeto, conforme a criterios empresariales.

Para el cumplimiento de su objeto, la entidad pública empresarial podrá realizar toda clase de actos de administración y disposición previstos en la legislación civil y mercantil. Asimismo, podrá realizar cuantas actividades comerciales o industriales estén relacionadas con dicho objeto, conforme a lo acordado por sus órganos de gobierno. Podrá actuar, incluso, mediante sociedades por ella participadas.

La entidad pública empresarial Red.es contará además con las siguientes funciones:

a) La gestión del registro de los nombres y direcciones de dominio de internet bajo el código de país correspondiente a España (.es), de acuerdo con la política de registros que se determine por el Ministerio de Industria, Energía y Turismo y en la normativa correspondiente.

b) La participación en los órganos que coordinen la gestión de Registros de nombre y dominios de la Corporación de Internet para la Asignación de Nombres y Números (ICANN), o la organización que en su caso la sustituya, así como el asesoramiento al Ministerio de Industria, Energía y Turismo en el Comité Asesor Gubernamental de ICANN (GAC) y, en general cuando le sea solicitado, el asesoramiento a la Administración General del Estado en el resto de los organismos internacionales y, en particular, en la Unión Europea, en todos los temas de su competencia.

c) La de observatorio del sector de las telecomunicaciones y de la sociedad de la información.

d) La elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la sociedad de la información, de conformidad con las instrucciones que dicte el Ministerio de Industria, Energía y Turismo.

e) El fomento y desarrollo de la Sociedad de la Información.

4. El régimen de contratación, de adquisición y de enajenación de la entidad se acomodará a las normas establecidas en derecho privado, sin perjuicio de lo determinado en el texto refundido de la Ley de Contratos del Sector Público, aprobado por el real decreto Legislativo 3/2011, de 14 de noviembre.

5. El régimen patrimonial de la entidad pública empresarial se ajustará a las previsiones del artículo 56 de la Ley 6/1997. No obstante, los actos de disposición y enajenación de los bienes que integran su patrimonio se regirán por el derecho privado. En especial, la entidad pública empresarial Red.es podrá afectar sus activos a las funciones asignadas a la misma en la letra e) del apartado tercero de esta disposición y a financiar transitoriamente el déficit de explotación resultante entre los ingresos y gastos correspondientes a las funciones asignadas en las letras a), b), c) y d) del mismo apartado.

6. La contratación del personal por la entidad pública empresarial se ajustará al derecho laboral, de acuerdo con las previsiones contenidas en el artículo 55 de la Ley 6/1997, debiéndose respetar, en cualquier caso, los principios de igualdad, mérito y capacidad.

7. El régimen presupuestario, el económico-financiero, el de contabilidad, el de intervención y el de control financiero de la entidad pública empresarial será el establecido en la Ley General Presupuestaria, de acuerdo con lo previsto en el artículo 58 y en la disposición transitoria tercera de la Ley 6/1997.

8. Los recursos económicos de la entidad podrán provenir de cualquiera de los enumerados en el apartado 1 del artículo 65 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Entre los recursos económicos de la entidad pública empresarial Red.es se incluyen los ingresos provenientes de lo recaudado en concepto del precio público por las operaciones de registro relativas a los nombres de dominio de Internet bajo el código de país correspondiente a España «.es» regulado en el apartado siguiente.

9. Precios Públicos por asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es».

La contraprestación pecuniaria que se satisfaga por la asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España tendrán la consideración de precio público.

Red.es, previa autorización del Ministerio de Industria, Energía y Turismo, establecerá mediante la correspondiente Instrucción, las tarifas de los precios públicos por la asignación,

renovación y otras operaciones de registro de los nombres de dominio bajo el «.es». La propuesta de establecimiento o modificación de la cuantía de precios públicos irá acompañada, de conformidad con lo previsto en el artículo 26 de la Ley 8/1989, de 13 de abril, que regula el Régimen Jurídico de las Tasas y Precios Públicos, de una memoria económico-financiera que justificará el importe de los mismos que se proponga y el grado de cobertura financiera de los costes correspondientes.

La gestión recaudatoria de los precios públicos referidos en este apartado corresponde a la entidad pública empresarial Red.es que determinará el procedimiento para su liquidación y pago mediante la Instrucción mencionada en el párrafo anterior en la que se establecerán los modelos de declaración, plazos y formas de pago.

La entidad pública empresarial Red.es podrá exigir la anticipación o el depósito previo del importe total o parcial de los precios públicos por las operaciones de registro relativas a los nombres de dominio «.es».

Disposición adicional decimoséptima. *Innovación en el ámbito de las tecnologías de la información y las comunicaciones.*

El Gobierno desarrollará un plan con medidas para potenciar la innovación en el ámbito de las tecnologías de la información y las comunicaciones, que permitan asimismo aprovechar el esfuerzo inversor que, en los próximos años, se llevará a cabo en el despliegue de las redes ultrarrápidas. El citado plan contemplará, entre otras, las siguientes actuaciones:

a) Promover la puesta en marcha de un foro de colaboración entre los operadores y la industria para identificar y potenciar las oportunidades que, para la industria electrónica y el resto de la industria, genere el despliegue de redes ultrarrápidas.

b) Estimular las políticas de innovación en el sector y la innovación tecnológica en el tejido industrial en colaboración con todos los agentes que intervienen en el desarrollo o crecimiento.

c) El establecimiento de medidas para potenciar las compras innovadoras y el mercado de demanda temprana para la puesta en marcha de proyectos de I + D + I relacionados con las tecnologías de la información y las comunicaciones.

Disposición adicional decimoctava. *Universalización de la banda ancha ultrarrápida.*

El Gobierno establecerá una Estrategia Nacional de Redes Ultrarrápidas que tenga como objetivo impulsar el despliegue de redes de acceso ultrarrápido a la banda ancha, tanto fijo como móvil, de cara a lograr su universalización, así como fomentar su adopción por ciudadanos, empresas y administraciones, para garantizar la cohesión social y territorial.

La Estrategia adoptará las medidas precisas para alcanzar los objetivos concretos de cobertura y adopción establecidos por la Agenda Digital para Europa e incorporados a la Agenda Digital para España y, en particular, para lograr la universalización de una conexión que permita comunicaciones de datos de banda ancha que se extenderá progresivamente, de forma que en el año 2017 alcanzará una velocidad mínima de Internet de 10 Mbps y antes de finalizar el año 2020 alcanzará a todos los usuarios a una velocidad mínima de Internet de 30 Mbps, y que al menos el 50% de los hogares puedan disponer de acceso a servicios de velocidades superiores a 100 Mbps. En el desarrollo de esta iniciativa de universalización de la banda ancha se evaluará la actualización del ámbito del servicio universal en relación con este servicio, atendiendo, en todo caso, a la normativa y orientaciones de la Unión Europea a este respecto.

La Estrategia establecerá la elaboración de un informe de cobertura de banda ancha ultrarrápida que permita conocer de forma precisa la situación de provisión de los servicios de comunicaciones electrónicas de banda ancha y que permita identificar aquellas zonas donde existan brechas de mercado.

La Estrategia contemplará políticas para incrementar la adopción y uso de la banda ancha ultrarrápida entre ciudadanos, empresas y administraciones. En particular se contemplarán las actuaciones necesarias para promover, de forma prioritaria, que los Centros de Salud comarcales, las Universidades Públicas, los Centros de Secundaria públicos y todas las Bibliotecas Públicas en la ciudad y comarcales, tengan en el año 2016

una conexión a la red pública de comunicaciones con capacidad de acceso funcional a Internet a una velocidad mínima de 30 Mpbs y de 100 Mbps en el año 2020. Estas medidas se articularán con la debida colaboración y coordinación con las Comunidades Autónomas.

Al menos una vez al año, el Ministerio de Industria, Energía y Turismo, informará al Parlamento sobre la adopción y cumplimiento de la Estrategia Nacional de Redes Ultrarrápidas y, en especial, sobre la evolución del despliegue de las redes ultrarrápidas y el cumplimiento de los objetivos de universalización de este servicio.

Disposición adicional decimonovena. *Estaciones radioeléctricas de radioaficionado.*

En la instalación de estaciones radioeléctricas de radioaficionado se aplicará lo establecido en la disposición adicional tercera de la Ley 12/2012, de 26 de diciembre, de medidas urgentes de liberalización del comercio y de determinados servicios, sin perjuicio de la aplicación de la Ley 19/1983, de 16 de noviembre, sobre regulación del derecho a instalar en el exterior de los inmuebles las antenas de las estaciones radioeléctricas de aficionados, y su normativa de desarrollo.

Disposición transitoria primera. *Normativa anterior a la entrada en vigor de esta Ley.*

Las normas reglamentarias en materia de telecomunicaciones vigentes con anterioridad a la entrada en vigor de la presente Ley o dictadas en desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones continuarán vigentes en lo que no se opongan a esta Ley, hasta que se apruebe su normativa de desarrollo.

Disposición transitoria segunda. *Adaptación de los operadores controlados directa o indirectamente por administraciones públicas al régimen previsto en el artículo 9.*

Los operadores controlados directa o indirectamente por administraciones públicas habrán de ajustarse a lo dispuesto en el artículo 9, en un plazo máximo de un año desde la entrada en vigor de la presente Ley.

Disposición transitoria tercera. *Condiciones ligadas a las concesiones de uso de dominio público radioeléctrico.*

Las condiciones ligadas a los títulos habilitantes para la explotación de redes o prestación de servicios de telecomunicaciones que implicaran el uso del dominio público radioeléctrico y que se hubieran otorgado con anterioridad a la entrada en vigor de la presente Ley a través de procedimientos de licitación pública, ya estuvieran previstas en los pliegos reguladores de las licitaciones o en la oferta del operador, pasan a estar ligadas a las concesiones de uso privativo de dominio público radioeléctrico.

Disposición transitoria cuarta. *Restricciones a los principios de neutralidad tecnológica y de servicios en los títulos habilitantes para el uso del espectro radioeléctrico para la prestación de servicios de comunicaciones electrónicas.*

1. Las condiciones establecidas en los títulos habilitantes para el uso del espectro radioeléctrico para la prestación de servicios de comunicaciones electrónicas otorgados con anterioridad al 25 de mayo de 2011 y que impliquen restricciones a los principios de neutralidad tecnológica y de servicios en los términos establecidos en el artículo 66 de esta Ley, seguirán siendo válidas hasta el 25 de mayo de 2016.

2. No obstante lo anterior, los titulares de títulos habilitantes para el uso del espectro radioeléctrico para la prestación de servicios de comunicaciones electrónicas cuyo periodo de vigencia se extienda más allá del 25 de mayo de 2016, podrán solicitar a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, antes del 25 de mayo de 2016, una evaluación de las restricciones a los principios de neutralidad tecnológica y de servicios en los términos establecidos en el artículo 66 de esta Ley, que tengan impuestas en sus títulos habilitantes.

Antes de dictar resolución, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información notificará al titular del título habilitante su nueva evaluación de

las restricciones, indicando el alcance de su título a raíz de ella y le concederá un plazo de 15 días hábiles para retirar su solicitud.

Si el titular del título desistiese de su solicitud, las restricciones a los principios de neutralidad tecnológica y de servicios establecidas en el título habilitante permanecerían sin modificar hasta el 25 de mayo de 2016, salvo que el título se extinga con anterioridad.

3. A partir del 25 de mayo de 2016, los principios de neutralidad tecnológica y de servicios se aplicarán a todos los títulos habilitantes para el uso del espectro para la prestación de servicios de comunicaciones electrónicas otorgados con anterioridad al 25 de mayo de 2011, sin perjuicio de las restricciones que puedan establecerse en los términos establecidos en el artículo 66 de esta Ley.

4. En la aplicación de esta disposición se tomarán las medidas apropiadas para fomentar la competencia leal.

5. Las medidas que se adopten en ejecución de esta disposición no tendrán en ningún caso la consideración de otorgamiento de un nuevo título habilitante.

Disposición transitoria quinta. *Prestación de determinados servicios a los que se refiere el artículo 28.*

La Sociedad Estatal Correos y Telégrafos, S.A., prestará directamente los servicios de télex, telegráficos y otros servicios de comunicaciones electrónicas de características similares, a los que se refiere el artículo 28.2 de esta Ley, ajustándose, en su caso, a lo que prevea el real decreto previsto en el apartado 3 de dicho artículo.

Asimismo, se encomienda a la Dirección General de la Marina Mercante la prestación de los servicios de seguridad de la vida humana en el mar subsumibles bajo el artículo 28.1.

Disposición transitoria sexta. *Régimen transitorio para la fijación de las tasas establecidas en el anexo I de esta Ley.*

Hasta que por la Ley de Presupuestos Generales del Estado se fijen las cuantías de la tasa prevista en el apartado 4 del Anexo I de esta Ley, se aplicarán las siguientes:

a) Por la expedición de certificaciones registrales, 42,51 euros.

b) Por la expedición de certificaciones de presentación a la administración de las telecomunicaciones del proyecto técnico de infraestructuras comunes de telecomunicaciones, el acta de replanteo, el boletín de instalación y el protocolo de pruebas y, en su caso, el certificado de fin de obra y sus anexos, 42,51 euros.

c) Por la expedición de certificaciones de cumplimiento de especificaciones técnicas, 335,49 euros.

d) Por cada acto de inspección previa o comprobación técnica efectuado, 352,72 euros.

e) Por la presentación de cada certificación expedida por técnico competente sustitutiva del acto de inspección previa, 88 euros.

f) Por la tramitación de la autorización o concesión demanial para el uso privativo del dominio público radioeléctrico, 68,46 euros.

g) Por la tramitación de la autorización de uso especial del dominio público radioeléctrico por los radioaficionados, 111 euros.

h) Por la presentación a los exámenes de capacitación para operar estaciones de radioaficionado, 22,98 euros.

i) Por inscripción en el registro de empresas instaladoras de telecomunicación, 104,54 euros.

j) Por la solicitud y emisión del dictamen técnico de evaluación de la conformidad de equipos y aparatos de telecomunicación, 345,82 euros.

Disposición transitoria séptima. *Solicitudes de autorizaciones o licencias administrativas efectuadas con anterioridad.*

1. Los procedimientos iniciados con anterioridad a la entrada en vigor de la presente Ley, y que tengan por finalidad la obtención de las licencias o autorizaciones de obra, instalaciones, de funcionamiento o de actividad, o de carácter medioambiental u otras de clase similar o análogas que fuesen precisas con arreglo a la normativa anterior, se

tramitarán y resolverán por la normativa vigente en el momento de la presentación de la solicitud.

2. No obstante lo dispuesto en el apartado anterior, el interesado podrá, con anterioridad a la resolución, desistir de su solicitud y, de este modo, optar por la aplicación de la nueva normativa en lo que ésta a su vez resultare de aplicación.

Disposición transitoria octava. *Registro de operadores.*

A la entrada en vigor de la presente Ley, se mantiene la inscripción de los datos que figuren en el Registro de operadores regulado en el artículo 7 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Disposición transitoria novena. *Adaptación de la normativa y los instrumentos de planificación territorial o urbanística elaborados por las administraciones públicas competentes que afecten al despliegue de las redes públicas de comunicaciones electrónicas.*

La normativa y los instrumentos de planificación territorial o urbanística elaborados por las administraciones públicas competentes que afecten al despliegue de las redes públicas de comunicaciones electrónicas deberán adaptarse a lo establecido en los artículos 34 y 35 en el plazo máximo de un año desde la entrada en vigor de la presente Ley.

Disposición transitoria décima. *Desempeño transitorio de funciones por la Comisión Nacional de los Mercados y la Competencia.*

En relación con las funciones que eran competencia de la Comisión Nacional de los Mercados y la Competencia y que, conforme a lo establecido en esta Ley, se atribuyen al Ministerio de Industria, Energía y Turismo, la Comisión Nacional de los Mercados y la Competencia las desempeñará hasta la fecha que se determine para el ejercicio efectivo de las nuevas funciones que esta Ley atribuye al Ministerio de Industria, Energía y Turismo conforme a lo establecido en la disposición adicional decimoquinta.

Disposición transitoria undécima. *Procedimientos iniciados con anterioridad a la entrada en vigor de esta Ley.*

Los procedimientos que versen sobre las funciones que eran competencia de la Comisión Nacional de los Mercados y la Competencia y que esta Ley atribuye al Ministerio de Industria, Energía y Turismo, y que se hayan iniciado con anterioridad a la fecha para el ejercicio efectivo de las nuevas funciones a que se refiere la disposición adicional decimoquinta, continuarán tramitándose por dicho Ministerio una vez que se cumpla dicha fecha.

Disposición transitoria duodécima. *Régimen transitorio de las estaciones o infraestructuras radioeléctricas para la prestación de servicios de comunicaciones electrónicas disponibles para el público para cuya instalación se hubiera presentado solicitud de licencia o autorización.*

Las estaciones o infraestructuras radioeléctricas para la prestación de servicios de comunicaciones electrónicas disponibles para el público para cuya instalación se hubiera solicitado la licencia o autorización previa de instalaciones, de funcionamiento, de actividad, de carácter medioambiental u otras de clase similar o análogas a las que se refiere el artículo 34.6, podrán continuar instaladas y en funcionamiento, sin perjuicio de que las administraciones públicas competentes puedan ejercer las potestades administrativas de comprobación, inspección, sanción y, en general, de control, que tengan atribuidas y que están referidas en el citado artículo 34.6 así como en el artículo 5 de la Ley 12/2012, de 26 de diciembre, de Medidas Urgentes de Liberalización del Comercio y Determinados Servicios.

No obstante, y de conformidad con lo prevenido en la disposición transitoria de la mencionada Ley 12/2012, de 26 de diciembre, los prestadores de servicios de comunicaciones electrónicas para el público que hubieren solicitado las licencias o

autorizaciones anteriormente mencionadas, sin perjuicio de la continuidad y funcionamiento de las respectivas instalaciones, podrán desistir de dichas solicitudes en curso y optar por presentar declaraciones responsables o, en su caso, comunicaciones previas de cambio de titularidad en los términos previstos en la citada Ley.

El ejercicio de las potestades administrativas de comprobación, inspección, sanción y, en general, de control deberá respetar los parámetros y requerimientos técnicos esenciales necesarios para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas mencionados en el artículo 34.4 y en la disposición adicional undécima.

Disposición derogatoria única. *Derogación normativa.*

Sin perjuicio de lo dispuesto en las disposiciones transitorias de esta Ley, quedan derogadas las siguientes disposiciones:

a) La Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

b) La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

c) Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 13/2011, de 27 de mayo, de regulación del juego.*

La Ley 13/2011, de 27 de mayo, de regulación del juego, queda modificada como sigue:

Uno. Se modifica el apartado 3 del artículo 7, que queda redactado en los siguientes términos:

> «3. Cualquier entidad, red publicitaria, agencia de publicidad, prestador de servicios de comunicación audiovisual o electrónica, medio de comunicación o servicio de la sociedad de la información que difunda la publicidad y promoción directa o indirecta de juegos o de sus operadores, deberá constatar que quien solicite la inserción de los anuncios o reclamos publicitarios dispone del correspondiente título habilitante expedido por la autoridad encargada de la regulación del juego y que éste le autoriza para la realización de la publicidad solicitada, absteniéndose de su práctica si careciera de aquél. La autoridad encargada de la regulación del juego, a través de su página web, mantendrá actualizada y accesible la información sobre los operadores habilitados.
>
> Se considera red publicitaria a la entidad que, en nombre y representación de los editores, ofrece a los anunciantes la utilización de espacios publicitarios en servicios de la sociedad de la información y la optimización de los resultados publicitarios al orientar los anuncios al público interesado por el producto o servicio publicitado.»

Dos. Se modifica el apartado 4 del artículo 7, que queda redactado en los siguientes términos:

> «4. La autoridad encargada de la regulación del juego en el ejercicio de la potestad administrativa de requerir el cese de la publicidad de las actividades de juego, se dirigirá a la entidad, red publicitaria, agencia de publicidad, prestador de servicios de comunicación audiovisual o electrónica, medio de comunicación, servicio de la sociedad de la información o red publicitaria correspondiente, indicándole motivadamente la infracción de la normativa aplicable.
>
> La entidad, red publicitaria, agencia de publicidad, prestador de servicios de comunicación audiovisual o electrónica, medio de comunicación, servicio de la sociedad de la información o red publicitaria deberá, en los tres días naturales siguientes a su recepción, comunicar el cumplimiento del requerimiento. En caso de que el mensaje publicitario cuente con un informe de consulta previa positivo emitido por un sistema de autorregulación publicitaria con el que la autoridad encargada de la regulación del juego tenga un convenio de colaboración de los previstos en el apartado 5 del artículo 24 de esta Ley, se entenderá que se actuó de buena fe si se

hubiese sujetado a dicho informe de consulta previa positivo, para el supuesto de actuación administrativa realizada en el marco de un expediente sancionador.»

Tres. Se modifica el apartado 8 del artículo 21, que queda redactado en los siguientes términos:

«8. Perseguir el juego no autorizado, ya se realice en el ámbito del Estado español, ya desde fuera de España y que se dirija al territorio del Estado, pudiendo requerir a cualquier proveedor de servicios de pago, entidades de prestación de servicios de comunicación audiovisual, medios de comunicación, servicios de la sociedad de la información o de comunicaciones electrónicas, agencias de publicidad y redes publicitarias, información relativa a las operaciones realizadas por los distintos operadores o por organizadores que carezcan de título habilitante o el cese de los servicios que estuvieran prestando.»

Cuatro. Se modifica el apartado 3 del artículo 36, que queda redactado en los siguientes términos:

«3. En particular, los prestadores de servicios de comunicación audiovisual, de comunicación electrónica y de la sociedad de la información, los medios de comunicación, así como las agencias de publicidad y las redes publicitarias serán responsables administrativos de la promoción, patrocinio y publicidad de los juegos a los que se refiere la presente Ley cuando quienes los realicen carezcan de título habilitante o cuando se difundan sin disponer de la autorización para publicitarlos o al margen de los límites fijados en la misma o infringiendo las normas vigentes en esta materia. No obstante, serán responsables de la infracción prevista en el artículo 40 d) las redes publicitarias que sirvan publicidad a prestadores de servicios de la sociedad de la información. La responsabilidad de los servicios de la sociedad de la información será subsidiaria de la de las agencias y redes publicitarias, siempre y cuando estas últimas sean adecuadamente identificadas por el servicio de la sociedad de la información, previo requerimiento de la autoridad encargada de la regulación del juego, y dispongan de un establecimiento permanente en España.

La competencia para instruir los procedimientos y sancionar a los prestadores de servicios de comunicación audiovisual corresponde a la Comisión Nacional de los Mercados y la Competencia, aplicándose en estos casos el régimen sancionador previsto en la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, salvo la excepción prevista en el apartado anterior, respecto de las infracciones del artículo 40, letra e).»

Cinco. Se modifica el apartado e) del artículo 40, que queda redactado en los siguientes términos:

«e) El incumplimiento de los requerimientos de información o de cese de prestación de servicios dictados por la autoridad encargada de la regulación del juego que se dirijan a los proveedores de servicios de pago, prestadores de servicios de comunicación audiovisual, prestadores de servicios de la sociedad de la información o de comunicaciones electrónicas, medios de comunicación social, agencias de publicidad y redes publicitarias.»

Disposición final segunda. *Modificación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, queda modificada como sigue:

Uno. Se modifica el apartado 1 f) del artículo 10, que queda redactado en los siguientes términos:

«f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.»

Dos. Se modifica el apartado 1 del artículo 18, que queda redactado como sigue:

«1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta que afecten a los consumidores y usuarios estarán sujetos, además, al capítulo V de la Ley 3/1991, de 10 de enero, de competencia desleal.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.»

Tres. Los apartados 1 y 3 del artículo 20 quedan redactados del siguiente modo:

«1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.»

«3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo.»

Cuatro. El apartado 2 del artículo 21 queda redactado del siguiente modo:

«2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.»

Cinco. El artículo 22 queda redactado en los siguientes términos:

«Artículo 22. *Derechos de los destinatarios de servicios.*

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que

los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.»

Seis. Se modifica el apartado 1 del artículo 35, que queda redactado como sigue:

«1. El Ministerio de Industria, Energía y Turismo controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.»

Siete. El artículo 37 queda redactado como sigue:

«Artículo 37. *Responsables.*

Los prestadores de servicios de la sociedad de la información están sujetos al régimen sancionador establecido en este título cuando la presente Ley les sea de aplicación.

Cuando las infracciones previstas en el artículo 38.3 i) y 38.4 g) se deban a la instalación de dispositivos de almacenamiento y recuperación de la información como consecuencia de la cesión por parte del prestador del servicio de la sociedad de la información de espacios propios para mostrar publicidad, será responsable de la infracción, además del prestador del servicio de la sociedad de la información, la red publicitaria o agente que gestione directamente con aquel la colocación de anuncios en dichos espacios en caso de no haber adoptado medidas para exigirle el cumplimiento de los deberes de información y la obtención del consentimiento del usuario.»

Ocho. El apartado 3 c) del artículo 38 queda redactado como sigue:

«c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.»

Nueve. El apartado 3 i) del artículo 38 queda redactado como sigue:

«i) La reincidencia en la comisión de la infracción leve prevista en el apartado 4 g) cuando así se hubiera declarado por resolución firme dictada en los tres años inmediatamente anteriores a la apertura del procedimiento sancionador.»

Diez. Se modifica el párrafo g) del artículo 38.4, que queda redactado como sigue:

«g) Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2.»

Once. Se introduce un nuevo artículo 39 bis con el siguiente contenido:

«Artículo 39 bis. *Moderación de sanciones.*

1. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 40.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el órgano competente no hubiese sancionado o apercibido con anterioridad al infractor como consecuencia de la comisión de infracciones previstas en esta Ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.»

Doce. Se modifica el artículo 40, que queda redactado como sigue:

«Artículo 40. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

a) La existencia de intencionalidad.
b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.
c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.
d) La naturaleza y cuantía de los perjuicios causados.
e) Los beneficios obtenidos por la infracción.
f) Volumen de facturación a que afecte la infracción cometida.
g) La adhesión a un código de conducta o a un sistema de autorregulación publicitaria aplicable respecto a la infracción cometida, que cumpla con lo dispuesto en el artículo 18 o en la disposición final octava y que haya sido informado favorablemente por el órgano u órganos competentes.»

Trece. Se modifica el artículo 43, que queda redactado como sigue:

«1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Energía y Turismo, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta

Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses.»

Catorce. Se introduce un apartado Cinco bis en la disposición adicional sexta, que queda redactado de la siguiente forma:

«Cinco bis. La autoridad de asignación suspenderá cautelarmente o cancelará, de acuerdo con el correspondiente requerimiento judicial previo, los nombres de dominio mediante los cuales se esté cometiendo un delito o falta tipificado en el Código Penal. Del mismo modo procederá la autoridad de asignación cuando por las Fuerzas y Cuerpos de Seguridad del Estado se le dirija requerimiento de suspensión cautelar dictado como diligencia de prevención dentro de las 24 horas siguientes al conocimiento de los hechos.

Asimismo, de acuerdo con lo dispuesto en los artículos 8, 11 y concordantes de esta Ley, la autoridad administrativa o judicial competente como medida para obtener la interrupción de la prestación de un servicio de la sociedad de la información o la retirada de un contenido, podrá requerir a la autoridad de asignación para que suspenda cautelarmente o cancele un nombre de dominio.

De la misma forma se procederá en los demás supuestos previstos legalmente.

En los supuestos previstos en los dos párrafos anteriores, sólo podrá ordenarse la suspensión cautelar o la cancelación de un nombre de dominio cuando el prestador de servicios o persona responsable no hubiera atendido el requerimiento dictado para el cese de la actividad ilícita.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá requerir la suspensión cautelar o la cancelación. En particular, cuando dichas medidas afecten a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrán ser decididas por los órganos jurisdiccionales competentes.

La suspensión consistirá en la imposibilidad de utilizar el nombre de dominio a los efectos del direccionamiento en Internet y la prohibición de modificar la titularidad y los datos registrales del mismo, si bien podrá añadir nuevos datos de contacto. El titular del nombre de dominio únicamente podrá renovar el mismo o modificar la modalidad de renovación. La suspensión cautelar se mantendrá hasta que sea levantada o bien, confirmada en una resolución definitiva que ordene la cancelación del nombre de dominio.

La cancelación tendrá los mismos efectos que la suspensión hasta la expiración del período de registro y si el tiempo restante es inferior a un año, por un año adicional, transcurrido el cual el nombre de dominio podrá volver a asignarse.»

Quince. Se introduce una nueva disposición adicional octava con el siguiente contenido:

«Disposición adicional octava. *Colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas.*

1. Los registros de nombres de dominio establecidos en España estarán sujetos a lo establecido en el apartado Cinco bis de la disposición adicional sexta, respecto de los nombres de dominio que asignen.

2. Las entidades de registro de nombres de dominio establecidas en España estarán obligadas a facilitar los datos relativos a los titulares de los nombres de dominio que soliciten las autoridades públicas para el ejercicio de sus competencias

de inspección, control y sanción cuando las infracciones administrativas que se persigan tengan relación directa con la actividad de una página de Internet identificada con los nombres de dominio que asignen.

Tales datos se facilitarán así mismo, cuando sean necesarios para la investigación y mitigación de incidentes de ciberseguridad en los que estén involucrados equipos relacionados con un nombre de dominio de los encomendados a su gestión. Dicha información será proporcionada al órgano, organismo o entidad que se determine legal o reglamentariamente.

En ambos supuestos, la solicitud deberá formularse mediante escrito motivado en el que se especificarán los datos requeridos y la necesidad y proporcionalidad de los datos solicitados para el fin que se persigue. Si los datos demandados son datos personales, su cesión no precisará el consentimiento de su titular.»

Dieciséis. Se introduce una disposición adicional novena con el siguiente contenido:

«Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por

el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.»

Disposición final tercera. *Modificación de la Ley 38/1999, de 5 de noviembre, de Ordenación de la Edificación.*

Se introduce la disposición adicional octava en la Ley 38/1999, de 5 de noviembre, de Ordenación de la Edificación, con el siguiente texto:

«Disposición adicional octava. *Instalación de infraestructuras de red o estaciones radioeléctricas en edificaciones de dominio privado.*

Las obras de instalación de infraestructuras de red o estaciones radioeléctricas en edificaciones de dominio privado no requerirán la obtención de licencia de obras o edificación ni otras autorizaciones, si bien, en todo caso el promotor de las mismas habrá de presentar ante la autoridad competente en materia de obras de edificación una declaración responsable donde conste que las obras se llevarán a cabo según un proyecto o una memoria técnica suscritos por técnico competente, según corresponda, justificativa del cumplimiento de los requisitos aplicables del Código Técnico de la Edificación. Una vez ejecutadas y finalizadas las obras de instalación de las infraestructuras de las redes de comunicaciones electrónicas, el promotor deberá presentar ante la autoridad competente una comunicación de la finalización de las obras y de que las mismas se han llevado a cabo según el proyecto técnico o memoria técnica.»

Disposición final cuarta. *Modificación de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, queda modificada como sigue:

Uno. Se modifica el apartado 2 del artículo 6, que queda redactado en los siguientes términos:

«2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.»

Dos. Se modifica el apartado 3 del artículo 7, que queda redactado en los siguientes términos:

«3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.»

Tres. Se modifica el artículo 10, que queda redactado en los siguientes términos:

«Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.»

Cuatro. Se modifica el apartado 5 de la disposición adicional única, que queda redactado en los siguientes términos:

«Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.»

Disposición final quinta. *Modificación del real decreto-ley 1/1998, de 27 de febrero, sobre infraestructuras comunes en los edificios para el acceso a los servicios de telecomunicación.*

Se modifica el apartado 1 del artículo 3 del real decreto-ley 1/1998, de 27 de febrero, sobre infraestructuras comunes en los edificios para el acceso a los servicios de telecomunicación, que queda redactado en los siguientes términos:

«1. A partir de la fecha de entrada en vigor del presente real decreto-ley, no se concederá autorización para la construcción o rehabilitación integral de ningún edificio de los referidos en el artículo 2, si al correspondiente proyecto arquitectónico no se une el que prevea la instalación de una infraestructura común propia. Esta infraestructura deberá reunir las condiciones técnicas adecuadas para cumplir, al menos, las funciones indicadas en el artículo 1.2 de este real decreto-ley, sin perjuicio de los que se determine en las normas que, en cada momento, se dicten en su desarrollo.

La instalación de la infraestructura regulada en este real decreto-ley debe contar con el correspondiente proyecto técnico, firmado por quien esté en posesión de un título universitario oficial de ingeniero, ingeniero técnico, máster o grado que tenga competencias sobre la materia en razón del plan de estudios de la respectiva titulación.

Mediante real decreto se determinará el contenido mínimo que debe tener dicho proyecto técnico.»

Disposición final sexta. *Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

El artículo 8.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, queda redactado como sigue:

«2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cinco años.»

Disposición final séptima. *Modificación de la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual.*

La Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, se modifica como sigue:

Uno. Se modifica el primer párrafo del apartado 2 del artículo 5 que queda redactado del siguiente modo:

«2. Para la efectividad de este derecho, los prestadores del servicio de comunicación televisiva de cobertura estatal o autonómica deben reservar a obras europeas el 51 por ciento del tiempo de emisión anual de su programación. A su vez, el 50 por ciento de esa cuota queda reservado para obras europeas en cualquiera de las lenguas españolas. En todo caso, el 10 por ciento del tiempo de emisión estará reservado a obras europeas de productores independientes del prestador de servicio y la mitad de ese 10 por ciento debe haber sido producida en los últimos cinco años. El tiempo de emisión a que se refiere este número se computará con exclusión del dedicado a informaciones, manifestaciones deportivas, juegos, publicidad, servicios de teletexto y televenta.»

Dos. Se modifica el artículo 17 que queda redactado del siguiente modo:

«1. Los prestadores del servicio de comunicación audiovisual tienen el derecho a realizar a cambio de contraprestación emplazamiento de productos en largometrajes, cortometrajes, documentales, películas y series de televisión, programas deportivos y programas de entretenimiento.

En los casos en que no se produzca pago alguno, sino únicamente el suministro gratuito de determinados bienes o servicios, tales como ayudas materiales a la producción o premios, con miras a su inclusión en un programa, únicamente constituirá emplazamiento de producto y por tanto estará permitido, siempre que estos bienes o servicios tengan un valor significativo.

2. Cuando el programa haya sido producido o encargado por el prestador del servicio o una de sus filiales, el público debe ser claramente informado del emplazamiento del producto al principio y al final del programa, y cuando se reanude tras una pausa publicitaria.

3. El emplazamiento no puede condicionar la responsabilidad ni la independencia editorial del prestador del servicio de comunicación audiovisual. Tampoco puede incitar directamente la compra o arrendamientos de bienes o servicios, realizar promociones concretas de éstos o dar prominencia indebida al producto.

4. Queda prohibido el emplazamiento de producto en la programación infantil».

Tres. Se modifica el artículo 38 que queda redactado del siguiente modo:

«Artículo 38. *Libertad de recepción de los servicios prestados dentro de la Unión Europea.*

1. Se garantiza la libertad de recepción en todo el territorio español de los servicios audiovisuales cuyos titulares se encuentren establecidos en un Estado miembro de la Unión Europea, siempre que no interfieran técnicamente en las emisiones de los prestadores establecidos bajo jurisdicción española. En el ámbito del Convenio Europeo sobre Televisión Transfronteriza y para canalizar el derecho a la diversidad cultural y lingüística a nivel europeo, en todas las zonas limítrofes con un país de la Unión Europea se posibilitará la emisión y la recepción de programas difundidos mediante ondas hertzianas garantizando para ello una adecuada planificación del espectro radioeléctrico en las zonas transfronterizas.

2. La autoridad audiovisual competente estatal, con carácter excepcional y de conformidad con lo dispuesto en el artículo 3 de la Directiva 2010/13, podrá limitar dicha libertad de recepción cuando los servicios audiovisuales televisivos procedentes de un Estado miembro de la Unión Europea infrinjan de manera grave y reiterada lo dispuesto en la legislación española en materia de protección de menores o contengan incitaciones al odio por razón de raza, sexo, religión o nacionalidad, siempre que esos servicios hubieran incurrido en las conductas anteriores al menos dos veces en los doce meses inmediatamente anteriores.

La autoridad audiovisual, en estos casos, y antes de adoptar las medidas de limitación, deberá notificar al titular de los servicios audiovisuales y a la Comisión Europea las infracciones alegadas y las medidas que tiene intención de adoptar en

caso de que se produzca de nuevo dicha infracción e iniciará consultas con ésta última y con el Estado miembro en el que el titular de los servicios audiovisuales esté establecido a fin de llegar a un arreglo amistoso.

Si las consultas con los sujetos mencionados en el apartado anterior no hubieran resultado en acuerdo y persistieran las infracciones, en un plazo de quince días a partir de la notificación de las mismas, podrán adoptarse las medidas previstas en el primer párrafo de este número.

En caso de decisión negativa por parte de la Comisión, se deberá poner fin urgentemente a las medidas de que se trate.

3. Además, si el servicio de comunicación audiovisual es a petición, la libertad de recepción podrá limitarse de forma proporcionada por razones de orden público, seguridad pública, protección de la salud pública, o para proteger a los consumidores e inversores. En este caso, antes de adoptar las medidas, la autoridad audiovisual deberá solicitar al Estado miembro de la Unión Europea a cuya jurisdicción esté sujeto el prestador de servicios a petición, que tome medidas y notificar, caso de que este último no las haya tomado, o no hayan sido suficientes, a la Comisión Europea y al Estado miembro señalado su intención de adoptarlas.

En casos de urgencia, la autoridad audiovisual podrá adoptar estas medidas notificando las mismas a la mayor brevedad a la Comisión Europea y al Estado miembro a cuya jurisdicción esté sujeto el prestador de servicios, indicando las razones de la urgencia.

En caso de decisión negativa por parte de la Comisión, la autoridad audiovisual deberá de abstenerse de adoptar las medidas propuestas o, en su caso, deberá poner fin urgentemente a las medidas de que se trate.

4. La acreditación de las medidas referidas en los dos números anteriores deberá efectuarse mediante la instrucción del correspondiente expediente por la autoridad audiovisual competente estatal.»

Cuatro. Se modifica el artículo 39 que queda redactado del siguiente modo:

«1. La autoridad competente estatal de conformidad con lo dispuesto en el artículo 4 de la Directiva 2010/13 podrá adoptar medidas de salvaguarda de la legislación española, de acuerdo con el procedimiento previsto en este artículo cuando el prestador de un servicio de comunicación audiovisual televisivo establecido en otro Estado miembro de la Unión Europea dirija su servicio total o principalmente al territorio español y se hubiera establecido en ese Estado miembro para eludir las normas españolas más estrictas.

En este caso, la autoridad competente estatal podrá ponerse, mediante petición debidamente motivada en contacto con el otro Estado miembro mencionado para lograr una solución de los problemas planteados que resulte mutuamente satisfactoria.

2. Si en el plazo de dos meses desde la petición no se alcanzase una solución satisfactoria, la autoridad competente estatal podrá adoptar las medidas previstas en el número uno de este artículo siempre que sean objetivamente necesarias y se apliquen de manera no discriminatoria y proporcionadas a los objetivos que se persiguen.

3. Con carácter previo a la adopción de las citadas medidas, la autoridad audiovisual deberá notificar a la Comisión Europea y al Estado miembro en el que se encuentre establecido el prestador del servicio de comunicación audiovisual televisivo, el proyecto de medidas a aplicar, al que se acompañará la justificación correspondiente. El proyecto de medida deberá ser aprobado por la Comisión Europea y en caso de decisión negativa por parte de ésta, la autoridad audiovisual se abstendrá de adoptar las medidas propuestas.»

Disposición final octava. *Regulación de las condiciones en que los órganos o entes gestores de infraestructuras de transporte de competencia estatal permitirán la ocupación del dominio público que gestionan y de la propiedad privada de que son titulares.*

A los efectos de lo previsto en los artículos 29 y 30 de la presente Ley, mediante real decreto acordado en Consejo de Ministros, a propuesta conjunta del Ministerio de Industria, Energía y Turismo y del Ministerio de Fomento, se determinarán las condiciones en que los órganos o entes gestores de infraestructuras de transporte de competencia estatal deben permitir el ejercicio del derecho de ocupación del dominio público que gestionan y de la propiedad privada de que son titulares, por los operadores de redes y servicios de comunicaciones electrónicas bajo los principios del acceso efectivo a dichos bienes, la reducción de cargas, y la simplificación administrativa, en condiciones equitativas, no discriminatorias, objetivas y neutrales.

Disposición final novena. *Fundamento constitucional.*

Esta Ley se dicta al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21.ª de la Constitución. Asimismo, las disposiciones de la Ley dirigidas a garantizar la unidad de mercado en el sector de las telecomunicaciones, se dictan al amparo del artículo 149.1.1.ª de la Constitución, sobre regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y del artículo 149.1.13.ª de la Constitución, sobre bases y coordinación de la planificación general de la actividad económica.

Disposición final décima. *Competencias de desarrollo.*

El Gobierno y el Ministro de Industria, Energía y Turismo, de acuerdo con lo previsto en esta Ley y en el ámbito de sus respectivas competencias, podrán dictar las normas reglamentarias que requieran el desarrollo y la aplicación de esta Ley.

Disposición final undécima. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Tasas en materia de telecomunicaciones

1. Tasa general de operadores

1. Sin perjuicio de la contribución económica que pueda imponerse a los operadores para la financiación del servicio universal, de acuerdo con lo establecido en el artículo 25 y en el Título III, todo operador estará obligado a satisfacer una tasa anual que no podrá exceder el 1,5 por mil de sus ingresos brutos de explotación y que estará destinada a sufragar los gastos que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta Ley, por las autoridades nacionales de reglamentación a que se refiere el artículo 68.

A efectos de lo señalado en el párrafo anterior, se entiende por ingresos brutos el conjunto de ingresos que obtenga el operador derivados de la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas incluidos en el ámbito de aplicación de esta Ley. A tales efectos, no se considerarán como ingresos brutos los correspondientes a servicios prestados por un operador cuyo importe recaude de los usuarios con el fin de remunerar los servicios de operadores que exploten redes o presten servicios de comunicaciones electrónicas.

2. La tasa se devengará el 31 de diciembre de cada año. No obstante, si por causa imputable al operador, éste perdiera la habilitación para actuar como tal en fecha anterior al 31 de diciembre, la tasa se devengará en la fecha en que esta circunstancia se produzca.

3. El importe de esta tasa anual no podrá exceder de los gastos que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta Ley, anteriormente referidos.

A tal efecto, el Ministerio de Industria, Energía y Turismo hará público antes del 30 de abril de cada año una memoria que contenga los gastos en que han incurrido en el ejercicio anterior las autoridades nacionales de reglamentación a que se refiere el artículo 68 por la aplicación del régimen jurídico establecido en esta Ley.

La memoria contemplará, de forma separada, los gastos en los que haya incurrido la Comisión Nacional de los Mercados y la Competencia por la aplicación del régimen jurídico establecido en esta Ley, que servirán de base para fijar la asignación anual de la Comisión con cargo a los Presupuestos Generales del Estado y garantizar la suficiencia de recursos financieros de la Comisión para la aplicación de esta Ley.

El importe de la tasa resultará de aplicar al importe de los gastos en que han incurrido en el ejercicio anterior las autoridades nacionales de reglamentación a que se refiere el artículo 68 por la aplicación del régimen jurídico establecido en esta Ley y que figura en la citada memoria, el porcentaje que individualmente representan los ingresos brutos de explotación de cada uno de los operadores de telecomunicaciones en el ejercicio anterior sobre el total de los ingresos brutos de explotación obtenidos en ese mismo ejercicio por los operadores de telecomunicaciones.

Mediante real decreto se determinará el sistema para calcular los gastos en que han incurrido las autoridades nacionales de reglamentación a que se refiere el artículo 68 por la aplicación del régimen jurídico establecido en esta Ley, el sistema de gestión para la liquidación de esta tasa y los plazos y requisitos que los operadores de telecomunicaciones deben cumplir para declarar al Ministerio de Industria, Energía y Turismo el importe de sus ingresos brutos de explotación con el objeto de que éste calcule el importe de la tasa que corresponde satisfacer a cada uno de los operadores de telecomunicaciones.

Si la referida declaración no se presentase en plazo, se formulará al sujeto pasivo requerimiento notificado con carácter fehaciente, a fin de que en el plazo de 10 días presente la declaración. Si no lo hiciera, el órgano gestor le girará una liquidación provisional sobre los ingresos brutos de la explotación determinados en régimen de estimación indirecta, conforme a lo dispuesto en el artículo 53 de la Ley 58/2003, de 17 de diciembre, General Tributaria, incluyendo, el importe de la sanción y los intereses de demora que procedan. Respecto de la imposición de la sanción se estará a lo dispuesto en la citada Ley General Tributaria.

2. Tasas por numeración, direccionamiento y denominación

1. Constituye el hecho imponible de la tasa el otorgamiento de derechos de uso de números, direcciones o nombres.

Serán sujetos pasivos de la tasa las personas físicas o jurídicas beneficiarias de derechos de uso.

La tasa se devengará el 1 de enero de cada año, excepto la del período inicial, que se devengará en la fecha que se produzca el otorgamiento de los derechos de uso.

El procedimiento para su exacción se establecerá por real decreto. El importe de dicha exacción será el resultado de multiplicar la cantidad de números, direcciones o nombres cuyos derechos de uso se hayan otorgado por el valor de cada uno de ellos, que podrá ser diferente en función de los servicios y planes correspondientes.

Con carácter general, el valor de cada número del Plan nacional de numeración telefónica para la fijación de la tasa por numeración, direccionamiento y denominación incluyendo a estos efectos los números empleados exclusivamente para la prestación de servicios de mensajes sobre redes telefónicas, será de 0,04 euros. A este valor se le aplicarán los coeficientes que se especifican en la siguiente tabla, para los rangos y servicios que se indican:

Coeficiente	Servicio	Rango (NXYA)	Longitud (cifras)
0	Servicios de interés social.	0XY, 112, 10YA	3 y 4
0	Servicios armonizados europeos de valor social.	116 A (A = 0 y 1)	6

Coeficiente	Servicio	Rango (NXYA)	Longitud (cifras)
0	Uso interno en el ámbito de cada operador.	12YA (YA= 00 - 19) 22YA	Indefinida.
2	Mensajes sobre redes telefónicas.	2XYA (X ≠ 2) 3XYA 79YA 99YA	5 y 6
3	Numeración corta y prefijos.	1XYA (X≠1) 50YA	4, 5 y 6
1	Numeración geográfica y vocal nómada geográfica.	9XYA (X≠0) 8XYA (X≠0)	9
1	Numeración móvil.	6XYA 7XYA (X=1, 2, 3, 4)	9
1	Numeración vocal nómada.	5XYA (X=1)	9
1	Numeración de acceso a Internet.	908A 909A	9
10	Tarifas especiales.	80YA (Y=0, 3, 6, 7) 90YA (Y=0, 1, 2, 5, 7)	9
10	Numeración personal.	70YA	9
30	Consulta telefónica sobre números de abonado.	118 A (A= 1 - 9)	5
2	Comunicaciones máquina a máquina.	590 A	13

Nota: En la columna correspondiente a la identificación de rango, las cifras NXYA representan las primeras 4 cifras del número marcado. Las cifras X, Y, A pueden tomar todos los valores entre 0 y 9, excepto en los casos que se indique otra cosa. El guión indica que las cifras referenciadas pueden tomar cualquier valor comprendido entre los mostrados a cada lado del mismo (éstos incluidos).

El Plan nacional de numeración telefónica y sus disposiciones de desarrollo podrán introducir coeficientes a aplicar para los recursos de numeración que se atribuyan con posterioridad a la entrada en vigor de esta Ley, siempre que aquéllos no sobrepasen el valor de 30, exceptuando los supuestos en que se otorguen derechos de uso de números de 9 cifras a usuarios finales, en cuyo caso el valor máximo resultante de la tasa no podrá superar los 100 euros.

A los efectos del cálculo de esta tasa, se entenderá que todos los números del Plan nacional de numeración telefónica, y los empleados exclusivamente para la prestación de servicios de mensajes sobre redes telefónicas públicas, están formados por nueve dígitos. Cuando se otorguen derechos de uso de un número con menos dígitos, se considerará que se están otorgando derechos de uso para la totalidad de los números de nueve dígitos que se puedan formar manteniendo como parte inicial de éstos el número cuyos derechos de uso se otorgan. Cuando se otorguen derechos de uso de números de mayor longitud, se considerará que se están otorgando para la totalidad de los números de nueve dígitos que se puedan formar con las nueve primeras cifras de aquéllos.

Asimismo, se establecen las siguientes tasas por numeración, direccionamiento y denominación:

Tipo de número	Norma de referencia	Valor de cada código (euros)
Código de punto de señalización internacional (CPSI).	Recomendación UIT-T Q.708.	1.000
Código de punto de señalización nacional (CPSN).	Recomendación UIT-T Q.704.	10
Indicativo de red de datos (CIRD).	Recomendación UIT-T X.121.	1.000
Indicativo de red móvil Tetra (IRM).	Recomendación UIT-T E.218.	1.000
Código de operador de portabilidad (NRN).	Especificaciones técnicas de portabilidad.	1.000
Indicativo de red móvil (IRM).	Recomendación UIT-T E.212.	1.000

Estas nuevas tasas se aplicarán sin carácter retroactivo desde el 1 de enero del año siguiente a la aprobación de la presente Ley.

El valor de la tasa por numeración, direccionamiento y denominación se fijará anualmente en la Ley de Presupuestos Generales del Estado.

2. No obstante lo dispuesto en el epígrafe anterior, en la fijación del importe a satisfacer por esta tasa se podrá tomar en consideración el valor de mercado del uso de los números y

nombres cuyos derechos de uso se otorguen y la rentabilidad que de ellos pudiera obtener la persona o entidad beneficiaria, conforme a lo dispuesto en el artículo 19.

En este caso, en los supuestos de carácter excepcional en que así esté previsto en los planes nacionales o sus disposiciones de desarrollo y en los términos que en éstos se fijen, la cuantía anual de la tasa podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia y el tiempo de duración del otorgamiento del derecho de uso. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa.

3. Procederá la devolución del importe de la tasa por numeración que proporcionalmente corresponda, cuando se produzca la cancelación de la asignación de recursos de numeración a petición del interesado, durante el ejercicio anual que corresponda. Para ello, se seguirá el procedimiento establecido mediante real decreto.

4. El importe de los ingresos obtenidos por esta tasa se ingresará en el Tesoro Público y se destinará a la financiación de los gastos que soporte la Administración General del Estado en la gestión, control y ejecución del régimen jurídico establecido en esta Ley.

3. Tasa por reserva del dominio público radioeléctrico

1. La reserva para uso privativo o para uso especial por operadores de cualquier frecuencia del dominio público radioeléctrico a favor de una o varias personas o entidades se gravará con una tasa anual, en los términos que se establecen en este apartado.

Para la fijación del importe a satisfacer en concepto de esta tasa por los sujetos obligados, se tendrá en cuenta el valor de mercado del uso de la frecuencia reservada y la rentabilidad que de él pudiera obtener el beneficiario.

Para la determinación del citado valor de mercado y de la posible rentabilidad obtenida por el beneficiario de la reserva se tomarán en consideración, entre otros, los siguientes parámetros:

a) El grado de utilización y congestión de las distintas bandas y en las distintas zonas geográficas.

b) El tipo de servicio para el que se pretende utilizar la reserva y, en particular, si éste lleva aparejadas las obligaciones de servicio público recogidas en el Título III.

c) La banda o sub-banda del espectro que se reserve.

d) Los equipos y tecnología que se empleen.

e) El valor económico derivado del uso o aprovechamiento del dominio público reservado.

2. El importe a satisfacer en concepto de esta tasa será el resultado de multiplicar la cantidad de unidades de reserva radioeléctrica del dominio público reservado por el valor en euros que se asigne a la unidad. En los territorios insulares, la superficie a aplicar para el cálculo de las unidades radioeléctricas que se utilicen para la determinación de la tasa correspondiente se calculará excluyendo la cobertura no solicitada que se extienda sobre la zona marítima. A los efectos de lo dispuesto en este apartado, se entiende por unidad de reserva radioeléctrica un patrón convencional de medida, referido a la ocupación potencial o real, durante el período de un año, de un ancho de banda de un kilohercio sobre un territorio de un kilómetro cuadrado.

3. La cuantificación de los parámetros anteriores se determinará por Ley de Presupuestos Generales del Estado. La reducción del parámetro indicado en el párrafo b) del epígrafe 1 de este apartado de la tasa por reserva de dominio público radioeléctrico, que se determinará en la Ley de Presupuestos Generales del Estado, será de hasta el 75 por 100 del valor de dicho coeficiente para las redes y servicios de comunicaciones electrónicas que lleven aparejadas obligaciones de servicio público de los artículos 25 y 28, apartados 1 y 2, de esta Ley, o para el dominio público destinado a la prestación de servicios públicos en gestión directa o indirecta mediante concesión administrativa.

Asimismo, en la Ley a que se refiere el párrafo anterior se fijará:

a) La fórmula para el cálculo del número de unidades de reserva radioeléctrica de los distintos servicios radioeléctricos.

b) Los tipos de servicios radioeléctricos.

c) El importe mínimo a ingresar en concepto de tasa por reserva del dominio público radioeléctrico.

4. El pago de la tasa deberá realizarse por el titular de la reserva de dominio público radioeléctrico. Las estaciones meramente receptoras que no dispongan de reserva radioeléctrica estarán excluidas del pago de la tasa. El importe de la exacción será ingresado en el Tesoro Público.

5. El importe de la tasa habrá de ser satisfecho anualmente. Se devengará inicialmente el día del otorgamiento del título habilitante para el uso del demanio y, posteriormente, el día 1 de enero de cada año.

6. El procedimiento de exacción se establecerá mediante real decreto. El impago del importe de la tasa podrá motivar la suspensión o la pérdida del derecho a la ocupación del dominio público radioeléctrico, salvo cuando, en el procedimiento de impugnación en vía administrativa o contencioso-administrativa interpuesto contra la liquidación de la tasa, se hubiese acordado la suspensión del pago.

7. Las administraciones públicas estarán exentas del pago de esta tasa en los supuestos de reserva de dominio público radioeléctrico para la prestación de servicios obligatorios de interés general que tenga exclusivamente por objeto la defensa nacional, la seguridad pública y las emergencias, así como cualesquiera otros servicios obligatorios de interés general sin contrapartida económica directa o indirecta, como tasas, precios públicos o privados, ni otros ingresos derivados de dicha prestación, tales como los ingresos en concepto de publicidad. A tal efecto, deberán solicitar, fundamentadamente, dicha exención al Ministerio de Industria, Energía y Turismo. Asimismo, no estarán sujetos al pago los enlaces descendentes de radiodifusión por satélite, tanto sonora como de televisión.

4. Tasas de telecomunicaciones

1. La gestión precisa para el otorgamiento de determinadas concesiones y autorizaciones, inscripciones registrales, emisión de certificaciones, realización de actuaciones obligatorias de inspección, emisión de dictámenes técnicos y la realización de exámenes darán derecho a la exacción de las tasas compensatorias del coste de los trámites y actuaciones necesarias, con arreglo a lo que se dispone en los párrafos siguientes.

2. Constituye el hecho imponible de la tasa la gestión precisa por la Administración para la emisión de certificaciones registrales; para la presentación de proyecto técnico de infraestructuras común de telecomunicaciones y del certificado o boletín de instalación que ampara las infraestructuras comunes de telecomunicaciones en el interior de edificios; de cumplimiento de las especificaciones técnicas de equipos y aparatos de telecomunicaciones; así como la emisión de dictámenes técnicos de evaluación de la conformidad de estos equipos y aparatos; las inscripciones en el registro de empresas instaladoras de telecomunicación; las actuaciones inspectoras o de comprobación técnica que, con carácter obligatorio, vengan establecidas en esta Ley o en otras disposiciones con rango legal o la presentación de certificaciones expedidas por técnico competente sustitutivas de dichas actuaciones inspectoras o de comprobación; la tramitación de concesiones demaniales para el uso privativo del dominio público radioeléctrico y la tramitación de autorizaciones generales o individuales de uso especial de dicho dominio y la realización de los exámenes de capacitación para operar estaciones de radioaficionado.

3. Serán sujetos pasivos de la tasa, según los supuestos, la persona natural o jurídica que solicite la correspondiente certificación o dictamen técnico de evaluación; que presente al registro de empresas instaladoras de telecomunicación la correspondiente declaración responsable; que solicite una certificación de presentación del proyecto técnico de infraestructuras comunes de telecomunicaciones, el acta de replanteo, el boletín de instalación y el protocolo de pruebas y, en su caso, el certificado de fin de obras y los anexos; aquélla a la que proceda practicar las actuaciones inspectoras de carácter obligatorio o solicite la tramitación o concesiones demaniales para el uso privativo del dominio público radioeléctrico o la tramitación de autorizaciones, generales o individuales, de uso especial del dominio público radioeléctrico; la que se presente a los exámenes para la obtención del título de operador de estaciones de aficionado, así como la que presente

certificaciones expedidas por técnico competente sustitutivas de actuaciones inspectoras o de comprobación de carácter obligatorio.

4. La cuantía de la tasa se establecerá en la Ley de Presupuestos Generales del Estado. La tasa se devengará en el momento de la solicitud correspondiente. El rendimiento de la tasa se ingresará en el Tesoro Público. Mediante real decreto se establecerá la forma de liquidación de la tasa.

La realización de pruebas o ensayos para comprobar el cumplimiento de especificaciones técnicas tendrá la consideración de precio público cuando aquéllas puedan efectuarse por el interesado, opcionalmente, en centros dependientes de la Administración de cualquier Estado miembro de la Unión Europea, de la Administración española o en centros privados o ajenos a aquéllas, cuando dichas pruebas sean solicitadas por el interesado voluntariamente sin que venga obligado a ello por la normativa en vigor.

5. Estarán exentos del pago de la tasa de tramitación de autorizaciones individuales de uso especial de dominio público radioeléctrico aquellos solicitantes de dichas autorizaciones que cumplan 65 años en el año en que efectúen la solicitud, o que los hayan cumplido con anterioridad, así como los beneficiarios de una pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.

5. Gestión y recaudación en período voluntario de las tasas

El Ministerio de Industria, Energía y Turismo gestionará y recaudará en período voluntario las tasas de este anexo.

ANEXO II

Definiciones

1. Abonado: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios.

2. Acceso: la puesta a disposición de otro operador, en condiciones definidas y sobre una base exclusiva o no exclusiva, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas, incluyendo cuando se utilicen para el suministro de servicios de la sociedad de información o de servicios de contenidos de radiodifusión. Este término abarca, entre otros aspectos, los siguientes: el acceso a elementos de redes y recursos asociados que pueden requerir la conexión de equipos por medios fijos y no fijos (en particular, esto incluye el acceso al bucle local y a recursos y servicios necesarios para facilitar servicios a través del bucle local); el acceso a infraestructuras físicas, como edificios, conductos y mástiles; el acceso a sistemas informáticos pertinentes, incluidos los sistemas de apoyo operativos; el acceso a sistemas de información o bases de datos para prepedidos, suministros, pedidos, solicitudes de mantenimiento y reparación, y facturación; el acceso a la conversión del número de llamada o a sistemas con una funcionalidad equivalente; el acceso a redes fijas y móviles, en particular con fines de itinerancia; el acceso a sistemas de acceso condicional para servicios de televisión digital; así como el acceso a servicios de red privada virtual.

3. Agente económico: el fabricante, el representante autorizado, el importador y el distribuidor de equipos y aparatos de telecomunicación.

a) Distribuidor: toda persona física o jurídica de la cadena de suministro distinta del fabricante o el importador que comercializa un producto.

b) Fabricante: toda persona física o jurídica que fabrica un producto, o que manda diseñar o fabricar un producto y lo comercializa con su nombre o marca comercial.

c) Importador: toda persona física o jurídica establecida en la Unión Europea que introduce un producto de un tercer país en el mercado comunitario.

d) Representante autorizado: toda persona física o jurídica establecida en la Unión Europea que ha recibido un mandato por escrito de un fabricante para actuar en su nombre en relación con tareas específicas relativas a obligaciones de éste último en virtud de la legislación comunitaria correspondiente.

4. Atribución de frecuencias: la designación de una banda de frecuencias para su uso por uno o más tipos de servicios de radiocomunicación, cuando proceda, en las condiciones que se especifiquen.

5. Asignación de frecuencias: Autorización administrativa para que una estación radioeléctrica utilice una frecuencia o un canal radioeléctrico determinado en condiciones especificadas.

6. Autoridad Nacional de Reglamentación: el Gobierno, los departamentos ministeriales, órganos superiores y directivos y organismos públicos, que de conformidad con esta Ley ejercen las competencias que en la misma se prevén.

7. Bucle local o bucle de abonado de la red pública de comunicaciones electrónicas fija: el circuito físico que conecta el punto de terminación de la red a un dispositivo de distribución o instalación equivalente de la red pública de comunicaciones electrónicas fija.

8. Consumidor: cualquier persona física o jurídica que utilice o solicite un servicio de comunicaciones electrónicas disponible para el público para fines no profesionales.

9. Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

10. Derechos exclusivos: los derechos concedidos a una empresa por medio de un instrumento legal, reglamentario o administrativo que le reserve el derecho a prestar un servicio o a emprender una actividad determinada en una zona geográfica específica.

11. Derechos especiales: los derechos concedidos a un número limitado de empresas por medio de un instrumento legal, reglamentario o administrativo que, en una zona geográfica específica:

a) Designen o limiten, con arreglo a criterios que no sean objetivos, proporcionales y no discriminatorios, a dos o más el número de tales empresas autorizadas a prestar un servicio o emprender una actividad determinada, o

b) Confiera a una empresa o empresas, con arreglo a tales criterios, ventajas legales o reglamentarias que dificulten gravemente la capacidad de otra empresa de prestar el mismo servicio o emprender la misma actividad en la misma zona geográfica y en unas condiciones básicamente similares.

12. Dirección: cadena o combinación de cifras y símbolos que identifica los puntos de terminación específicos de una conexión y que se utiliza para encaminamiento.

13. Equipo avanzado de televisión digital: decodificadores para la conexión a televisores o televisores digitales integrados capaces de recibir servicios de televisión digital interactiva.

14. Equipo terminal: equipo destinado a ser conectado a una red pública de comunicaciones electrónicas, esto es, a estar conectado directamente a los puntos de terminación de aquélla o interfuncionar, a su través, con objeto de enviar, procesar o recibir información.

15. Especificación técnica: la especificación que figura en un documento que define las características necesarias de un producto, tales como los niveles de calidad o las propiedades de su uso, la seguridad, las dimensiones, los símbolos, las pruebas y los métodos de prueba, el empaquetado, el marcado y el etiquetado. Se incluyen dentro de la citada categoría las normas aplicables al producto en lo que se refiere a la terminología.

16. Espectro radioeléctrico: ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3.000 GHz, que se propagan por el espacio sin guía artificial.

17. Explotación de una red de comunicación electrónica: la creación, el aprovechamiento, el control o la puesta a disposición de dicha red.

18. Interconexión: la conexión física y lógica de las redes públicas de comunicaciones utilizadas por un mismo operador o por otro distinto, de manera que los usuarios de un operador puedan comunicarse con los usuarios del mismo operador o de otro distinto, o acceder a los servicios prestados por otro operador. Los servicios podrán ser prestados por las partes interesadas o por terceros que tengan acceso a la red. La interconexión constituye un tipo particular de acceso entre operadores de redes públicas.

19. Interfaz de programa de aplicación (API): la interfaz de software entre las aplicaciones externas, puesta a disposición por los operadores de radiodifusión o prestadores de servicios, y los recursos del equipo avanzado de televisión digital para los servicios de radio y televisión digital.

20. Interferencia perjudicial: toda interferencia que suponga un riesgo para el funcionamiento de un servicio de radionavegación o de otros servicios de seguridad o que degrade u obstruya gravemente o interrumpa de forma repetida un servicio de radiocomunicación que funcione de conformidad con la reglamentación internacional, comunitaria o nacional aplicable.

21. Llamada: una conexión establecida por medio de un servicio de comunicaciones electrónicas disponible para el público que permita la comunicación bidireccional de voz.

22. Nombre: combinación de caracteres (cifras decimales, letras o símbolos) que se utiliza para identificar abonados, usuarios u otras entidades tales como elementos de red.

23. Número: cadena de cifras decimales que, entre otros, pueden representar un nombre o una dirección.

24. Número geográfico: el número identificado en el plan nacional de numeración telefónica que contiene en parte de su estructura un significado geográfico utilizado para el encaminamiento de las llamadas hacia la ubicación física del punto de terminación de la red.

25. Números no geográficos: los números identificados en el plan nacional de numeración telefónica que no son números geográficos. Incluirán, entre otros, los números de teléfonos móviles, los de llamada gratuita y los de tarificación adicional.

26. Operador: persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado al Ministerio de Industria, Energía y Turismo el inicio de su actividad o está inscrita en el Registro de operadores.

27. Operador con poder significativo en el mercado: operador que, individual o conjuntamente con otros, disfruta de una posición equivalente a una posición dominante, esto es, una posición de fuerza económica que permite que su comportamiento sea, en medida apreciable, independiente de los competidores, los clientes y, en última instancia, los consumidores que sean personas físicas.

28. Punto de terminación de la red: el punto físico en el que el abonado accede a una red pública de comunicaciones. Cuando se trate de redes en las que se produzcan operaciones de conmutación o encaminamiento, el punto de terminación de la red estará identificado mediante una dirección de red específica, la cual podrá estar vinculada a un número o a un nombre de un abonado.

29. Radiocomunicación: toda telecomunicación transmitida por medio de ondas radioeléctricas.

30. Recursos asociados: las infraestructuras físicas, los sistemas, dispositivos, los servicios asociados u otros recursos o elementos asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen la prestación de servicios a través de dicha red o servicio o tengan potencial para ello. Incluirán, entre otros, edificios o entradas de edificios, el cableado de edificios, antenas, torres y otras construcciones de soporte, conductos, mástiles, bocas de acceso y distribuidores.

31. Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos que no son activos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

32. Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de señales entre puntos de terminación de la red.

33. Reserva de frecuencias: Porción de espectro radioeléctrico cuyos derechos de uso se otorgan por la Administración a una persona física o jurídica en condiciones especificadas.

34. Servicios asociados: aquellos servicios asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen el suministro de servicios a través de dicha red o servicio o tengan potencial para ello e incluyen, entre otros, la traducción de números o sistemas con una funcionalidad equivalente, los sistemas de acceso condicional y las guías electrónicas de programas, así como otros servicios tales como el servicio de identidad, localización y presencia.

35. Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.

36. Servicio de televisión de formato ancho: el servicio de televisión constituido, total o parcialmente, por programas producidos y editados para su presentación en formato ancho completo. La relación de dimensiones 16:9 constituye el formato de referencia para los servicios de televisión de este tipo.

37. Servicio telefónico disponible al público: el servicio disponible al público para efectuar y recibir, directa o indirectamente, llamadas nacionales o nacionales e internacionales a través de uno o más números de un plan nacional o internacional de numeración telefónica.

38. Sistema de acceso condicional: toda medida técnica o mecanismo técnico que condicione el acceso en forma inteligible a un servicio protegido de radiodifusión sonora o televisiva al pago de una cuota u otra forma de autorización individual previa.

39. Telecomunicaciones: toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

40. Teléfono público de pago: un teléfono accesible al público en general y para cuya utilización pueden emplearse como medios de pago monedas, tarjetas de crédito/débito o tarjetas de prepago, incluidas las tarjetas que utilizan códigos de marcación.

41. Usuario: una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público.

42. Usuario final: el usuario que no explota redes públicas de comunicaciones ni presta servicios de comunicaciones electrónicas disponibles para el público ni tampoco los revende.

§ 34

Real Decreto 863/2008, de 23 de mayo, por el que se aprueba el Reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico

Ministerio de Industria, Turismo y Comercio
«BOE» núm. 138, de 7 de junio de 2008
Última modificación: 16 de junio de 2015
Referencia: BOE-A-2008-9855

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, instauró un nuevo marco regulador en lo referente a la planificación y gestión del espectro radioeléctrico, introduciendo la regulación y tendencias comunitarias en la materia, esto es, la garantía del uso eficaz y eficiente del espectro radioeléctrico como principio superior que debe guiar la planificación y la asignación de frecuencias por la Administración y el uso de éstas por los operadores. Asimismo, esta Ley abre la posibilidad de la transferencia de títulos habilitantes y de la cesión de derechos de uso del espectro radioeléctrico en las condiciones que se determinen reglamentariamente. Además, establece, en su artículo 44, que el Gobierno desarrollará reglamentariamente las condiciones de gestión del dominio público radioeléctrico, la elaboración de los planes para su utilización y los procedimientos de otorgamiento de los derechos de uso de dicho dominio.

El Real Decreto 424/2005, de 15 de abril, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, mediante su disposición final primera modificó el reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico, aprobado por la Orden del Ministro de Fomento, de 9 de marzo de 2000, con el objetivo de adecuar su contenido al de la Ley General de Telecomunicaciones, en especial en los aspectos relativos a competencias y procedimientos.

La universalización de las comunicaciones y la aparición de nuevos servicios asociados al desarrollo de la sociedad de la información exigen una continua actualización de las técnicas y procedimientos relacionados con la planificación de redes y servicios de comunicaciones electrónicas. Las comunicaciones inalámbricas, que utilizan como soporte de transmisión el dominio público radioeléctrico, constituyen el pilar fundamental en el desarrollo de soluciones asociadas a la movilidad, socialmente cada día más demandadas.

Conceptos innovadores como mercado secundario, neutralidad tecnológica y de servicios, uso flexible, entre otros, deben ser considerados como criterios inspiradores a la hora de definir las mejores técnicas de planificación y gestión de un recurso como el dominio público radioeléctrico, limitado, pero cada día mas demandado y que sólo bajo la optimización de su uso podrá hacer frente a las nuevas necesidades de comunicaciones que la sociedad plantea.

El reglamento del uso del dominio público radioeléctrico constituye un documento regulatorio básico para el desarrollo y aplicación de criterios y procedimientos innovadores en materia de planificación y gestión de redes y servicios de comunicaciones inalámbricas, que debe incluir los planteamientos del marco regulador de las comunicaciones electrónicas en Europa y, en particular, lo dispuesto en la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas («Directiva marco»), la Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas («Directiva de autorización») y la Decisión número 676/2002/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea (Decisión espectro radioeléctrico).

Asimismo, se han tenido en cuenta en la elaboración de este reglamento las tendencias marcadas en la propuesta de la Comisión Europea de un nuevo marco regulador de las comunicaciones electrónicas en la Unión Europea hecha pública el día 13 de noviembre de 2007.

Para avanzar en la consecución de los objetivos anteriormente señalados, resulta preciso aprobar un nuevo reglamento regulador del uso del dominio público radioeléctrico.

En este nuevo reglamento se regula la puesta en funcionamiento de un Registro público de concesionarios de derechos de uso privativo del dominio público radioeléctrico, accesible a través de Internet, con el objetivo de aumentar la transparencia de los procesos de otorgamiento de derechos de uso del dominio público radioeléctrico, mediante la publicidad de las características técnicas y nombres de los titulares de los citados derechos, dando cumplimiento además a las exigencias de la Unión Europea en esta materia.

También se introducen modificaciones en los procedimientos para la obtención de recursos órbita-espectro.

Una de las principales novedades que se incorporan en el reglamento que se aprueba mediante el presente real decreto consiste en añadir, a la posibilidad existente actualmente de transferencia total del título habilitante, nuevas posibilidades de transferencia parcial del título y de cesión de derechos de uso del dominio público radioeléctrico respecto de una parte de las frecuencias o de una parte del ámbito geográfico.

Asimismo, y en relación con este apartado, el reglamento establece los derechos de uso que no son susceptibles de transmisión, las causas de revocación de la autorización de transmisión y la prohibición de realizar cesiones sucesivas y simultáneas. Como anexo al reglamento se incluye la relación de servicios con frecuencias reservadas en las bandas indicadas susceptibles de transferencia parcial o cesión a terceros de los derechos de uso del dominio público radioeléctrico.

Por último, cabe destacar el contenido de la disposición adicional segunda del reglamento, referente a la transformación de las concesiones de dominio público radioeléctrico vinculadas a los extintos títulos habilitantes con limitación de número para la prestación de diferentes servicios. Se establece que el procedimiento de transformación se iniciará de oficio y que en las resoluciones expresas por las que se transformen los títulos se establecerán los derechos y obligaciones que se declaran subsistentes de los títulos actuales, y que también podrán incluirse otras obligaciones por razones de servicio público e interés general, así como las que se consideren necesarias para preservar las condiciones de competencia en el mercado y las condiciones que resulten necesarias para su adecuación al presente reglamento, al Cuadro Nacional de Atribución de Frecuencias y a la normativa de la Unión Europea que, en su caso, resulte de aplicación, en especial, la referida a los principios de neutralidad tecnológica y de los servicios.

El presente real decreto ha sido objeto de informe por parte de la Comisión del Mercado de las Telecomunicaciones y del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información. De conformidad con lo establecido en la disposición adicional quinta de la Ley General de Telecomunicaciones, el informe de este último órgano equivale a la audiencia a la que se refiere el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta del Ministro de Industria, Turismo y Comercio, de acuerdo con el Consejo de Estado, previa aprobación de la Ministra de Administraciones Públicas y previa deliberación del Consejo de Ministros en su reunión del día 23 de mayo de 2008,

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico, que se inserta a continuación.

Disposición adicional única. *Protección de datos de carácter personal.*

El tratamiento de los datos relativos al registro nacional de frecuencias, el registro público de concesionarios y a los procedimientos de obtención de los títulos habilitantes para el uso privativo del dominio público radioeléctrico se encontrará sometido a lo dispuesto en Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus normas de desarrollo

Disposición transitoria primera. *Ejercicio de funciones hasta la constitución de la Agencia Estatal de Radiocomunicaciones.*

Las competencias y funciones administrativas que se atribuyen en este real decreto y el reglamento que aprueba a la Agencia Estatal de Radiocomunicaciones serán ejercidas por los órganos competentes del Ministerio de Industria, Turismo y Comercio hasta la efectiva constitución de la misma, momento en el que de conformidad con lo dispuesto en el artículo 47 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, pasará a corresponder su ejercicio a dicho organismo.

Disposición transitoria segunda. *Procedimientos iniciados con anterioridad a la entrada en vigor de este real decreto.*

Lo especificado en el presente real decreto y el reglamento que aprueba no será de aplicación a los procedimientos iniciados con anterioridad a la fecha de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden de 9 de marzo de 2000 por la que se aprueba el reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del espectro radioeléctrico, modificada por el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, con excepción de la disposición transitoria cuarta que mantendrá su vigencia hasta el cese de las emisiones de televisión terrestre con tecnología analógica, de conformidad con lo establecido en la disposición adicional primera del Real Decreto 944/2005, de 29 de julio, por el que se aprueba el plan técnico nacional de la televisión digital terrestre.

Quedan derogadas, igualmente, cuantas otras disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Facultades de desarrollo.*

Se autoriza al Ministro de Industria, Turismo y Comercio, en el ámbito de sus competencias, a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto, en especial, para modificar o actualizar el contenido del anexo del reglamento que se aprueba mediante este real decreto, así como la relación de bandas de frecuencias a la que hace referencia su disposición adicional primera. La modificación o actualización del contenido del anexo del reglamento que se aprueba mediante este real decreto, así como la relación de bandas de frecuencias a la que hace referencia su disposición adicional primera

se aprobará por orden del Ministro de Industria, Turismo y Comercio, previo acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos.

Asimismo, se autoriza a la Agencia Estatal de Radiocomunicaciones para aprobar los modelos de solicitud de títulos habilitantes para el uso del dominio público radioeléctrico, así como sus posibles modificaciones.

Disposición final segunda. *Título competencial.*

Este real decreto se dicta al amparo de la competencia exclusiva del Estado sobre telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY 32/2003, DE 3 DE NOVIEMBRE, GENERAL DE TELECOMUNI-CACIONES, EN LO RELATIVO AL USO DEL DOMINIO PÚBLICO RADIOELÉCTRICO

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente reglamento tiene por objeto el desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.

Artículo 2. *Objetivos y principios.*

Son objetivos y principios que inspiran el presente reglamento los siguientes:

a) Garantizar, mediante una gestión adecuada, el uso eficaz y eficiente del dominio público radioeléctrico.

b) Promover el uso del dominio público radioeléctrico como factor de desarrollo técnico, económico, de seguridad, del interés público, social y cultural.

c) Garantizar un acceso equitativo a los recursos radioeléctricos mediante procedimientos abiertos, transparentes, objetivos y no discriminatorios.

d) Promover el desarrollo y la utilización de nuevos servicios, redes y tecnologías, y el acceso a ellos de todos los ciudadanos.

e) Regular la transferencia de títulos habilitantes y la cesión a terceros de determinados derechos de uso del dominio público radioeléctrico.

f) Contribuir al desarrollo normativo armonizado en el ámbito de la Unión Europea que facilite la introducción de sistemas de comunicaciones globales.

g) Facilitar la planificación estratégica del sector de las telecomunicaciones y, en particular, de las comunicaciones relacionadas con la defensa nacional y de los servicios de protección civil y emergencias.

h) Fomentar la neutralidad tecnológica y de los servicios como elementos flexibilizadores en el uso eficiente del dominio público radioeléctrico.

i) Fomentar una mayor competencia en los mercados de comunicaciones electrónicas.

j) Promover una inversión eficiente en materia de infraestructuras y fomentar la innovación.

Artículo 3. *Concepto de dominio público radioeléctrico.*

1. A los efectos del presente reglamento, se considera dominio público radioeléctrico el espacio por el que pueden propagarse las ondas radioeléctricas. Se entiende por ondas

radioeléctricas las ondas electromagnéticas cuya frecuencia se fija convencionalmente por debajo de 3.000 gigahertzios que se propagan por el espacio sin guía artificial.

2. La utilización de ondas electromagnéticas de frecuencias superiores a 3.000 gigahertzios y propagadas por el espacio sin guía artificial se somete al mismo régimen que la utilización de las ondas radioeléctricas, siéndole de aplicación lo dispuesto en la Ley General de Telecomunicaciones y en el presente reglamento.

Artículo 4. *Planes de utilización del dominio público radioeléctrico.*

1. La utilización del dominio público radioeléctrico se efectuará de acuerdo con una planificación previa que delimite las bandas y canales atribuidos a cada uno de los servicios.

2. Son planes de utilización del dominio público radioeléctrico el Cuadro Nacional de Atribución de Frecuencias, los planes técnicos nacionales de radiodifusión sonora y de televisión y los aprobados por otras normas de igual o superior rango.

3. Corresponde a la Agencia Estatal de Radiocomunicaciones la elaboración de las propuestas de los planes de utilización del dominio público radioeléctrico y su tramitación, elevándolos al órgano competente para su aprobación.

TÍTULO II

Planificación del dominio público radioeléctrico

Artículo 5. *Cuadro Nacional de Atribución de Frecuencias.*

1. A fin de lograr la utilización coordinada y eficaz del dominio público radioeléctrico, el Ministro de Industria, Turismo y Comercio, a propuesta de la Agencia Estatal de Radiocomunicaciones, aprobará el Cuadro Nacional de Atribución de Frecuencias para los diferentes tipos de servicios de radiocomunicación, de acuerdo con las disposiciones de la Unión Europea, de la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), y del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), definiendo la atribución de bandas, subbandas, frecuencias, canales y los circuitos radioeléctricos correspondientes, así como las demás características técnicas que pudieran ser necesarias.

2. Asimismo, el Cuadro Nacional de Atribución de Frecuencias, de acuerdo con la reglamentación internacional sobre atribución y adjudicación de bandas y asignaciones de frecuencia, y con las disponibilidades nacionales e internacionales del espectro de frecuencias radioeléctricas y la demanda social, podrá establecer, entre otras, las siguientes previsiones:

a) La reserva de parte del dominio público radioeléctrico para servicios determinados.

b) Preferencias de uso por razón del fin social del servicio a prestar.

c) Delimitación de las bandas, canales o frecuencias que se reservan a las Administraciones Públicas o entes públicos de ellas dependientes para la gestión directa de sus servicios.

d) Previsión respecto de la explotación en el futuro de las distintas bandas de frecuencias, fomentando la neutralidad tecnológica y de los servicios.

3. En el proceso de elaboración del Cuadro Nacional de Atribución de Frecuencias será de aplicación el procedimiento de elaboración de disposiciones administrativas de carácter general. La Agencia Estatal de Radiocomunicaciones someterá a consulta pública los proyectos correspondientes.

Artículo 6. *Planes técnicos de radiodifusión y televisión.*

1. Corresponde a la Agencia Estatal de Radiocomunicaciones la elaboración de los proyectos de los planes técnicos nacionales de radiodifusión sonora y de televisión conforme al procedimiento establecido en este artículo.

2. El procedimiento se iniciará consultando a la Corporación de Radio y Televisión Española, (Corporación RTVE), a los Entes públicos de radio y televisión de las Comunidades Autónomas y a los órganos competentes en materia de radio y televisión de

las Comunidades Autónomas sobre sus necesidades de frecuencias. Asimismo, se consultará a las asociaciones más representativas de los operadores privados de radio o televisión, según el caso.

3. Los proyectos de los planes técnicos nacionales de radiodifusión sonora y de televisión serán elaborados teniendo en cuenta las necesidades de frecuencias planteadas por las entidades y organismos previamente consultados, con el objetivo de alcanzar una utilización racional, óptima y eficaz del dominio público radioeléctrico.

4. Los planes técnicos nacionales de radiodifusión sonora y de televisión establecerán, al menos, las frecuencias de emisión, los bloques de frecuencias o, en su caso, los canales radioeléctricos para proporcionar servicios de calidad técnica satisfactoria en las zonas de servicio expresamente definidas, así como cualesquiera otros parámetros técnicos de referencia o cualesquiera otras disposiciones administrativas que resulten necesarias.

5. En el proceso de elaboración de los planes técnicos nacionales de radiodifusión sonora y de televisión será de aplicación el procedimiento de elaboración de disposiciones de carácter general.

Artículo 7. *Registro Nacional de Frecuencias.*

1. La Agencia Estatal de Radiocomunicaciones gestionará un registro de usos de las frecuencias en todo el territorio nacional. En dicho registro se inscribirán, además de los datos del titular de cada asignación de frecuencias, las características técnicas de éstas.

2. Para garantizar la protección de los intereses comerciales y estratégicos de los titulares de derechos de uso del dominio público radioeléctrico y la protección de los datos personales, el acceso directo al registro quedará restringido a las personas que designe la Agencia Estatal de Radiocomunicaciones. Asimismo, para garantizar los intereses relacionados con la defensa nacional, el acceso directo al registro sobre los usos de las frecuencias vinculados a la misma quedará restringido a las personas que designen conjuntamente el Ministerio de Defensa y la Agencia Estatal de Radiocomunicaciones.

Artículo 8. *Registro público de concesionarios.*

La Agencia Estatal de Radiocomunicaciones, en el plazo máximo de seis meses a contar desde la fecha de entrada en vigor de este reglamento, pondrá en funcionamiento un registro público accesible a través de Internet, en el que se incluirán los siguientes datos de las concesiones administrativas en vigor para el uso privativo del dominio público radioeléctrico:

a) Referencia de la concesión.

b) Nombre o razón social, domicilio y número o código de identificación fiscal del titular.

c) Fecha de otorgamiento y caducidad de la concesión.

d) Ámbito geográfico y tipo de servicio autorizado.

e) Frecuencia o banda de frecuencias reservadas.

f) Indicación sobre si la concesión es susceptible de transferencia parcial o sobre si sus derechos de uso del dominio público radioeléctrico son susceptibles de cesión a terceros.

g) Indicación, en su caso, de si los derechos de uso del dominio público radioeléctrico han sido obtenidos mediante un procedimiento de transferencia de título, así como el nombre o razón social y el número o código de identificación fiscal del titular que transfiere el título.

h) Indicación, en su caso, de si los derechos de uso del dominio público radioeléctrico a que habilita la concesión es objeto de cesión por un periodo superior a seis meses así como el nombre o razón social y el número o código de identificación fiscal del titular al que se cede los derechos.

i) Indicación, en su caso, de que la concesión ha sido objeto de la transformación a la que se refiere la disposición adicional segunda.

TÍTULO III

Uso del dominio público radioeléctrico

CAPÍTULO I

Disposiciones comunes a los diferentes usos del dominio público radioeléctrico

Artículo 9. *Tipos de uso del dominio público radioeléctrico.*

El uso del dominio público radioeléctrico puede ser común, especial o privativo, quedando en todos los casos sometido a las disposiciones contenidas en este reglamento.

Artículo 10. *Uso eficaz y uso eficiente del dominio público radioeléctrico.*

1. A los efectos del presente reglamento, se entenderá que las asignaciones realizadas utilizan eficazmente el dominio público radioeléctrico cuando su uso sea progresivo, efectivo y continuado en las zonas geográficas para las que fue reservado, sin perjuicio de las reservas destinadas a situaciones de emergencia o relacionados con la defensa nacional.

2. Asimismo, se entenderá por uso eficiente del dominio público radioeléctrico aquel que proporciona un menor consumo de recursos espectrales garantizando los mismos objetivos de cobertura y calidad del servicio.

3. El uso eficaz y eficiente del dominio público radioeléctrico constituyen sendas condiciones permanentemente exigibles a los titulares de derechos de uso del dominio público durante la vigencia de los correspondientes títulos habilitantes. La Agencia Estatal de Radiocomunicaciones, previa tramitación del correspondiente expediente administrativo de acuerdo con lo establecido en el artículo 25 de este reglamento, podrá modificar las condiciones asociadas a los títulos habilitantes para el uso del dominio público en lo que se refiere a la cantidad de espectro, a la zona geográfica para la que fue reservado o a las características técnicas de uso, a fin de asegurar un uso eficaz del dominio público radioeléctrico y unos niveles adecuados de eficiencia.

CAPÍTULO II

Uso común y uso especial del dominio público radioeléctrico

Artículo 11. *Concepto y régimen jurídico del uso común del dominio público radioeléctrico.*

1. Tendrá la consideración de uso común del dominio público radioeléctrico:

a) La utilización de aquellas bandas, subbandas o frecuencias que se señalen en el Cuadro Nacional de Atribución de Frecuencias como de uso común, con las características técnicas especificadas en dicho cuadro.

b) La utilización de aquellas bandas, subbandas y frecuencias que se señalen en el Cuadro Nacional de Atribución de Frecuencias para aplicaciones industriales, científicas y médicas (ICM).

2. Asimismo, tendrán la consideración de uso común, los enlaces de comunicaciones mediante ondas electromagnéticas con frecuencias correspondientes al espectro visible (enlaces ópticos).

3. Los servicios que efectúen un uso común del dominio público radioeléctrico no deberán producir interferencias ni para ellos se podrá solicitar protección frente a servicios de comunicaciones electrónicas autorizados.

4. El uso común del dominio público radioeléctrico no precisará de título habilitante y se ejercerá con sujeción a lo dispuesto en este reglamento.

Artículo 12. *Concepto de uso especial del dominio público radioeléctrico.*

Tendrá la consideración de uso especial del dominio público radioeléctrico el que se lleve a cabo en las bandas, subbandas y frecuencias que se señalen como de uso compartido, sin exclusión de terceros, y no considerado como de uso común, por radioaficionados o para fines de mero entretenimiento u ocio sin contenido económico, como los de la banda ciudadana.

Artículo 13. *Título habilitante para el uso especial del dominio público radioeléctrico.*

1. De acuerdo con el artículo 45 de la Ley General de Telecomunicaciones, la utilización de aquellas partes del dominio público radioeléctrico que el Cuadro Nacional de Atribución de Frecuencias delimite como de uso especial exigirá previamente la obtención de una autorización administrativa individualizada en los términos, condiciones y plazos que se establezcan mediante orden ministerial.

2. Dicha autorización se otorgará por orden de presentación de solicitudes sin más limitaciones que las que se deriven de la de policía y buena gestión del dominio público radioeléctrico, sin perjuicio de derechos de terceros usuarios del dominio público.

3. La autorización de uso especial del dominio público radioeléctrico tendrá carácter personal y conservarán su vigencia mientras su titular no manifieste su renuncia a la misma. No obstante, y a efectos de planificación y control de las emisiones radioeléctricas, el titular tiene la carga de comunicar fehacientemente a la Agencia Estatal de Radiocomunicaciones, cada cinco años, su intención de seguir utilizando el dominio público radioeléctrico. El incumplimiento, en su caso, de esta carga será causa de extinción de la autorización, previa tramitación del correspondiente expediente administrativo, en el que se dará la oportunidad al interesado para que en el plazo de un mes subsane la omisión de la comunicación de su intención de seguir utilizando el dominio público radioeléctrico. Si el interesado subsana dicha omisión, no se podrá extinguir la autorización por esta causa.

4. Mediante orden ministerial se establecerán las condiciones de explotación del dominio público radioeléctrico bajo esta modalidad de uso. Asimismo, dicha orden regulará los plazos y procedimientos de aplicación de la carga de comunicación a la que hace referencia el párrafo anterior, pudiendo incluso establecer la supresión de dicha carga en función de la evolución de los servicios que llevan a cabo un uso especial del dominio público radioeléctrico.

Artículo 14. *Revocación de autorizaciones de uso especial del dominio público radioeléctrico.*

Son causas de revocación de la autorización de uso especial del dominio público radioeléctrico, previa tramitación del correspondiente expediente:

a) La utilización del dominio público radioeléctrico para fines distintos de los que se establezcan en la resolución de autorización.

b) El mal uso del dominio público que provoque alteraciones que impidan el uso por terceros que dispongan del correspondiente título habilitante.

c) El incumplimiento grave de las leyes y reglamentos de policía y gestión del dominio público radioeléctrico que, en su caso, regulen las normas a cumplir por los equipos y aparatos que lo utilicen para la protección de dicho dominio público.

d) La modificación del Cuadro Nacional de Atribución de Frecuencias, fundada en razones de disponibilidades y necesidades del dominio público radioeléctrico o en razones técnicas que alteren la clasificación de una banda, subbanda o frecuencia y establezca su carácter de uso privativo o para otros fines.

Artículo 15. *Limitación de los derechos de uso común y especial.*

Por razones de eficiencia en el uso del dominio público radioeléctrico o por razones técnicas de atribución de bandas, el Cuadro Nacional de Atribución de Frecuencias podrá modificar el carácter de uso común o especial en determinadas bandas, subbandas o frecuencias, y establecer su adscripción para uso privativo. En dicho supuesto, se señalará en la orden de modificación del Cuadro Nacional de Atribución de Frecuencias un período

transitorio de adaptación o amortización de equipos, no originando, en ningún caso, derecho de indemnización a los actuales usuarios.

TÍTULO IV

Uso privativo del dominio público radioeléctrico

CAPÍTULO I

Disposiciones generales

Artículo 16. *Frecuencias y servicios.*

1. Las asignaciones de frecuencias para el uso privativo del dominio público radioeléctrico se efectuarán, en cualquier caso, para la prestación de los servicios o el ejercicio de las actividades especificadas en el correspondiente título habilitante.

2. La utilización de las frecuencias con fines distintos a los que motivaron su asignación o para otros diferentes de los de la prestación del servicio o el ejercicio de la actividad que haya motivado su asignación facultará a la Agencia Estatal de Radiocomunicaciones para que proceda a su revocación, de conformidad con lo establecido en el artículo 28 de este reglamento.

Artículo 17. *Uso compartido del dominio público radioeléctrico.*

Los titulares de derechos de uso de frecuencias, bandas o subbandas del dominio público radioeléctrico que en el Cuadro Nacional de Atribución de Frecuencias se establezcan como de uso compartido con otros titulares habrán de aceptar las limitaciones y restricciones inherentes a dicho régimen de asignación de frecuencias, incorporando a sus redes los dispositivos técnicos pertinentes.

Artículo 18. *Títulos habilitantes para el uso privativo del dominio público radioeléctrico.*

1. De acuerdo con el artículo 45 de la Ley General de Telecomunicaciones, el otorgamiento del derecho de uso privativo del dominio público radioeléctrico revestirá alguna de las formas siguientes:

a) Autorización administrativa.
b) Afectación demanial.
c) Concesión administrativa.

2. En el caso de autoprestación de servicios por el solicitante, el derecho al uso privativo del dominio público radioeléctrico se obtendrá mediante autorización administrativa, salvo en el caso de Administraciones Públicas, en el que se obtendrá mediante afectación demanial. No se otorgarán derechos de uso privativo del dominio público radioeléctrico para su uso en autoprestación en los supuestos en los que la demanda supere a la oferta y se aplique el procedimiento previsto en el artículo 44.2 de la Ley General de Telecomunicaciones.

3. En los restantes supuestos, el derecho al uso privativo del dominio público radioeléctrico requerirá concesión administrativa. Para el otorgamiento de dicha concesión demanial, será requisito previo que los solicitantes se hallen inscritos en el Registro de Operadores de la Comisión del Mercado de las Telecomunicaciones como operadores del servicio para el que se solicita la concesión demanial.

Artículo 19. *Inspección previa al uso del dominio público radioeléctrico.*

1. De acuerdo con lo dispuesto en el artículo 45.4 de la Ley General de Telecomunicaciones, será requisito previo a la utilización del dominio público radioeléctrico la inspección o reconocimiento satisfactorio de las instalaciones por la Agencia Estatal de Radiocomunicaciones.

2. En función de la naturaleza del servicio, de la banda de frecuencias empleada, de la importancia técnica de las instalaciones que se utilicen o por razones de eficacia en la

gestión del dominio público, dicha inspección o reconocimiento previo podrá ser sustituida por la certificación expedida por técnico competente en materia de telecomunicaciones a la que se refiere el artículo 45.4 de la Ley General de Telecomunicaciones, certificación que deberá ser remitida a la Agencia Estatal de Radiocomunicaciones a efecto de que por la misma se pueda expedir la autorización de puesta en funcionamiento.

3. Mediante resolución del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información se establecerán las bandas de frecuencias o servicios en los que, conforme al apartado anterior, la inspección podrá ser sustituida por la certificación prevista en el mismo.

4. Previo reconocimiento o, en su caso, certificación favorable de las instalaciones, la Agencia Estatal de Radiocomunicaciones expedirá la autorización de puesta en funcionamiento de la red e inicio de la prestación efectiva del servicio.

CAPÍTULO II

Procedimientos de obtención y régimen jurídico de los títulos habilitantes para uso privativo del dominio público radioeléctrico

Sección 1.ª Procedimiento General

Artículo 20. *Presentación y tramitación de solicitudes y documentación anexa.*

1. Los interesados en obtener cualquier título habilitante para el uso privativo del dominio público radioeléctrico presentarán sus solicitudes, junto a la propuesta técnica, preferentemente ante la Agencia Estatal de Radiocomunicaciones o en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en el impreso formulario oficial que corresponda, debidamente cumplimentado, o bien a través de los registros telemáticos correspondientes conforme a la normativa vigente.

La solicitud deberá ir acompañada de la siguiente documentación:

a) Documentación administrativa, que estará integrada por los documentos que a continuación se relacionan y que podrán aportarse en original o copia compulsada:

1. Documentos que acrediten la capacidad del solicitante.

Si se trata de una persona física, fotocopia del documento nacional de identidad o, en el supuesto de extranjeros, la documentación equivalente que acredite la identidad y nacionalidad del interesado o, en su defecto, consentimiento para que los datos de identidad personal de éste puedan ser consultados mediante el Sistema de Verificación de Datos de Identidad Personal, a los efectos de iniciación del procedimiento, de conformidad con lo establecido en la Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al sistema de verificación de datos de identidad.

Tanto para personas físicas como jurídicas, el número de identificación fiscal o, cuando se trate de personas físicas o jurídicas extranjeras, el documento equivalente.

2. Documentos que acrediten la representación.

Los que comparezcan o firmen solicitudes en nombre de otros deberán presentar poder bastante al efecto, en su caso, debidamente inscrito en el Registro Mercantil, y el documento nacional de identidad o, en su caso, el consentimiento a la verificación de identidad indicado en el punto 1.

Si el solicitante fuese una persona física o jurídica extranjera, deberá designar una persona responsable a efectos de notificaciones domiciliada en España, sin perjuicio de lo que puedan prever los acuerdos internacionales.

3. Documentos que acrediten su condición de operador de comunicaciones electrónicas, en el caso de concesiones demaniales.

4. Justificante, en su caso, de abono de la tasa de telecomunicaciones establecida en el anexo I.4 de la Ley General de Telecomunicaciones.

5. Declaración de someterse a la jurisdicción de los juzgados y tribunales españoles de cualquier orden para todas las incidencias que, de modo directo o indirecto, pudieran surgir del título habilitante concedido, con renuncia, en su caso, al fuero jurisdiccional extranjero

que pudiera corresponder al solicitante. Los solicitantes españoles no deberán presentar esta declaración.

b) Propuesta técnica.-La propuesta técnica, firmada por técnico competente en materia de telecomunicaciones, describirá la solución técnica adoptada en función de las necesidades de radiocomunicaciones planteadas, especificando las características técnicas de la red que se pretenda instalar y cuanta otra información sea necesaria para definir el uso del dominio público radioeléctrico que se solicita.

La propuesta técnica se ajustará al modelo oficial establecido a tales efectos, incorporando planos topográficos de escala adecuada en los que figuren los emplazamientos de las estaciones fijas y la zona de servicio de la red a instalar. Cuando la complejidad del sistema de telecomunicación propuesto, por razón de utilización del dominio público o del servicio a prestar, lo hiciere aconsejable, la Agencia Estatal de Radiocomunicaciones podrá exigir del peticionario la presentación del correspondiente proyecto técnico firmado por un técnico competente en materia de telecomunicaciones en el que se especifiquen tanto las características técnicas de los equipos y aparatos, como los estudios y cálculos de las necesidades de dominio público radioeléctrico planteadas y las características del servicio para el que se pretende utilizar.

2. La Agencia Estatal de Radiocomunicaciones, antes de dictar la resolución sobre el otorgamiento o denegación del título habilitante necesario para el uso privativo del dominio público radioeléctrico y en el plazo previsto para ello, podrá requerir al solicitante cuanta información o aclaraciones considere convenientes sobre su solicitud o sobre los documentos con ella presentados.

3. Cuando sea preciso para garantizar una gestión eficaz y eficiente del dominio público radioeléctrico, la Agencia Estatal de Radiocomunicaciones podrá modificar las características técnicas solicitadas previa audiencia del interesado y sin perjuicio del mantenimiento de los objetivos de servicio propuestos por el solicitante. En este supuesto, la validez del título otorgado estará condicionada a su aceptación por el solicitante.

4. La autorización de los emplazamientos de las estaciones fijas quedará condicionada, en cualquier caso, a la ausencia de perturbaciones a otros servicios radioeléctricos autorizados, así como al cumplimiento de las disposiciones vigentes en materia de zonas e instalaciones de interés para la Defensa Nacional, de servidumbres radioeléctricas o aeronáuticas, de medio ambiente, de ordenación del territorio o cualquier otra que le resulte de aplicación y, en todo caso, a lo establecido en el Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece las condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas. La obtención de los permisos o autorizaciones relacionados con estas materias será responsabilidad y correrá a cargo del titular de la autorización.

Artículo 21. *Plazos para notificar la resolución.*

1. El plazo para notificar la resolución expresa de las solicitudes de otorgamiento, modificación y extinción de títulos habilitantes para el uso privativo del dominio público radioeléctrico será de seis semanas desde la entrada de la solicitud en cualquiera de los registros de la Agencia Estatal de Radiocomunicaciones. No obstante, de conformidad con lo dispuesto en el artículo 44.1.d) de la Ley General de Telecomunicaciones, no será de aplicación dicho plazo cuando se precise alcanzar la coordinación internacional que, en su caso, proceda o afecte a la reserva de recursos órbita-espectro.

2. Transcurrido el plazo al que se refiere el apartado anterior sin que haya recaído resolución expresa, deberán entenderse desestimadas las solicitudes, sin perjuicio de la obligación de la Agencia Estatal de Radiocomunicaciones de resolver expresamente, de acuerdo con lo dispuesto en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Cuando el otorgamiento del título se produzca a través de un procedimiento de licitación, se estará a lo dispuesto en el artículo 29 de este reglamento.

Artículo 22. *Resolución del procedimiento.*

1. La Agencia Estatal de Radiocomunicaciones dictará resolución otorgando o denegando motivadamente el título solicitado. Dicha resolución pone fin a la vía administrativa.

2. Las resoluciones en virtud de las cuales se otorguen títulos habilitantes para el uso del dominio público radioeléctrico recogerán los parámetros técnicos de funcionamiento, los plazos de vigencia, la zona de servicio, el número de unidades de reserva radioeléctrica y cualquier otra condición que deban cumplir sus titulares.

3. Los titulares de concesiones y autorizaciones de uso privativo del dominio público radioeléctrico están obligados al pago del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados, conforme a su normativa reguladora.

4. A efectos de su inscripción en el Registro público de concesionarios al que hace referencia el artículo 8 de este reglamento, los titulares de concesiones demaniales deberán acreditar, en el plazo de tres meses desde la notificación, el pago del citado impuesto. Una vez se produzca dicha acreditación, la Agencia Estatal de Radiocomunicaciones dispondrá de un plazo de quince días para efectuar la citada inscripción. Transcurridos tres meses sin que se haya producido la acreditación, la concesión será revocada mediante resolución de la Agencia Estatal de Radiocomunicaciones conforme a lo establecido en el artículo 28 de este reglamento.

Artículo 23. *Denegación de solicitudes.*

La Agencia Estatal de Radiocomunicaciones podrá denegar las solicitudes por alguna de las siguientes causas:

a) Cuando el solicitante no tenga la condición de operador de comunicaciones electrónicas, en el caso de concesiones demaniales.

b) Insuficiencia de los documentos aportados.

c) Falta de adecuación de sus características técnicas al Cuadro Nacional de Atribución de Frecuencias.

d) Insuficiencia de dominio público radioeléctrico disponible en las bandas de frecuencia reservadas por el Cuadro Nacional de Atribución de Frecuencias para el servicio solicitado.

e) Falta de adecuación de las características técnicas solicitadas a los objetivos de cobertura de los servicios previstos, siempre que su titular no acepte las alternativas técnicas propuestas por la Agencia Estatal de Radiocomunicaciones.

f) Cuando se advierta que el número de interesados en la obtención de los derechos de uso es superior a la oferta de dominio público radioeléctrico.

Artículo 24. *Plazos de vigencia de los títulos habilitantes.*

1. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico se otorgarán por un período de tiempo inicial que finalizará el 31 de diciembre del año natural en que cumpla su quinto de vigencia, renovable por períodos sucesivos de cinco años previa solicitud de su titular.

2. Si el titular deseara renovar el título habilitante, deberá solicitarlo entre el 1 de septiembre y el 15 de noviembre del último año de vigencia.

3. Ante una solicitud de renovación, la Agencia Estatal de Radiocomunicaciones podrá:

a) Acordar la renovación solicitada sin modificar sus características técnicas.

b) Ofrecer al interesado la renovación solicitada introduciendo en el título las variaciones técnicas que requiera su adaptación al Cuadro Nacional de Atribución de Frecuencias.

c) Acordar su denegación por falta de adecuación al Cuadro Nacional de Atribución de Frecuencias o por cualquier otra causa de denegación de solicitud prevista en el artículo 23.

4. Si al concluir el período de vigencia del título, la Agencia Estatal de Radiocomunicaciones no se hubiera pronunciado sobre la solicitud de renovación, ésta se entenderá desestimada, sin perjuicio de la obligación de resolver expresamente de acuerdo con lo dispuesto en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En este caso, y hasta que la Agencia Estatal de Radiocomunicaciones dicte resolución expresa,

se entenderá prorrogado el derecho del titular al uso del dominio público radioeléctrico en las condiciones reguladas en el título para el que ha solicitado su renovación.

5. Los plazos de vigencia de los títulos habilitantes para el servicio de radiodifusión sonora y televisión se regirán por su normativa específica. Asimismo, para los títulos otorgados por un procedimiento de licitación se estará a lo establecido en los pliegos de bases por los que se rija el procedimiento, siendo preceptivo, en todo caso, el informe previo de la Comisión del Mercado de las Telecomunicaciones.

Artículo 25. *Modificación de los títulos habilitantes.*

1. La Agencia Estatal de Radiocomunicaciones podrá modificar, en cualquier momento, de oficio o a instancia de parte, durante el período de vigencia de un título habilitante que otorgue derechos de uso privativo sobre el dominio público radioeléctrico, sus características técnicas cuando ello sea preciso para su adecuación al Cuadro Nacional de Atribución de Frecuencias, por razones de uso eficaz y eficiente del dominio público radioeléctrico de acuerdo con lo previsto en el artículo 10 de este reglamento, o por obligaciones derivadas del cumplimiento de la normativa internacional o comunitaria.

2. A efectos de lo dispuesto en este artículo, se entenderá por modificación la alteración del ámbito geográfico, frecuencias, potencias, banda o cualquier otra característica técnica del título habilitante original, siempre que de la misma no se derive una imposibilidad de atender el fin para el que se venía utilizando el dominio público radioeléctrico reservado.

3. Mediante orden del Ministerio de Industria, Turismo y Comercio, previa audiencia de los interesados, de las asociaciones de usuarios, e informe preceptivo de la Comisión del Mercado de las Telecomunicaciones, y con respeto a la legislación sobre patrimonio de las Administraciones Públicas, se podrán modificar las condiciones generales a que se sujetan los títulos habilitantes para el uso privativo del dominio público radioeléctrico, con arreglo a los principios de objetividad y proporcionalidad, y atendiendo principalmente a las necesidades de la planificación y del uso eficaz y eficiente, y la disponibilidad del dominio público radioeléctrico.

Artículo 26. *Efectos de la modificación de los títulos habilitantes.*

1. Los daños y perjuicios que se deriven de la modificación de un título habilitante llevada a cabo por la Agencia Estatal de Radiocomunicaciones, sin mediar causa imputable a su titular, darán derecho a indemnización, salvo cuando vengan impuestas por normas internacionales o por el ordenamiento jurídico de la Unión Europea.

2. Tampoco darán derecho a indemnización las modificaciones que se produzcan con ocasión de cualesquiera de las renovaciones que en su caso se otorguen, siempre que estas modificaciones resulten necesarias para su adaptación al Cuadro Nacional de Atribución de Frecuencias.

Artículo 27. *Extinción de los títulos habilitantes.*

Los títulos habilitantes para el uso privativo del dominio público se extinguirán por:

a) Las causas que resulten aplicables de las reseñadas en el artículo 100 de la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas.

b) Muerte del titular del derecho de uso privativo del dominio público radioeléctrico o extinción de la persona jurídica titular.

c) Renuncia del titular, con efectos desde su aceptación por la Agencia Estatal de Radiocomunicaciones.

d) Pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico en caso de tratarse de concesiones de uso privativo, o cualquier causa que imposibilite la prestación del servicio por su titular.

e) Pérdida de adecuación de las características técnicas de la red al Cuadro Nacional de Atribución de Frecuencias, sin que exista posibilidad de otorgar al titular otras bandas, en cuyo caso éste tendrá derecho a indemnización conforme a lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

f) Mutuo acuerdo entre el titular y la Agencia Estatal de Radiocomunicaciones.

g) Transcurrido el tiempo para el que se otorgaron, sin que se haya presentado solicitud de renovación, comunicando tal extremo a los responsables de los registros correspondientes.

h) Por incumplimiento grave y reiterado de las obligaciones del titular contemplado como causa de revocación en el artículo siguiente.

i) Aquellas otras causas que se establezcan en el título habilitante, conforme a la Ley General de Telecomunicaciones.

Artículo 28. *Revocación de los títulos habilitantes.*

1. La Agencia Estatal de Radiocomunicaciones, a través del procedimiento administrativo general de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá acordar la revocación de los títulos habilitantes para uso privativo del dominio público radioeléctrico por las siguientes causas:

a) El incumplimiento de las condiciones y requisitos técnicos aplicables al uso privativo del dominio público radioeléctrico.

b) No pagar el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados.

c) No efectuar un uso eficaz o eficiente del dominio público radioeléctrico al que se refiere el artículo 10 de este reglamento.

d) La revocación sucesiva de dos autorizaciones administrativas de transferencia de título o de cesión de derechos de uso del dominio público radioeléctrico sobre el mismo título habilitante en el plazo de un año, en los términos establecidos en el artículo 44.

e) La utilización de las frecuencias con fines distintos a los que motivaron su asignación o para otros diferentes de los de la prestación del servicio o el ejercicio de la actividad que haya motivado su asignación.

2. Cuando la Agencia Estatal de Radiocomunicaciones compruebe que el titular del título habilitante incurre en alguna causa de revocación, le notificará esta circunstancia a su titular, concediéndole la oportunidad de subsanar el posible incumplimiento o de manifestar su opinión en los siguientes plazos:

a) Un mes a contar desde la notificación.

b) Un plazo inferior acordado por la Agencia Estatal de Radiocomunicaciones, nunca inferior a quince días, en caso de repetidos incumplimientos.

c) Un plazo superior acordado por la Agencia Estatal de Radiocomunicaciones cuando, por causas objetivas, lo estime oportuno.

3. Si el titular no subsana los incumplimientos en el plazo a que se refiere el apartado anterior, la Agencia Estatal de Radiocomunicaciones propondrá al Ministerio de Industria, Turismo y Comercio la incoación de un expediente sancionador dirigido a la imposición de una multa económica, que se tramitará conforme a lo dispuesto en el Título VIII de la Ley General de Telecomunicaciones.

4. En todo caso, cuando la Agencia Estatal de Radiocomunicaciones constate que el incumplimiento en que incurre el titular representa una amenaza inmediata y grave para la seguridad pública o la salud pública, o que cree graves problemas económicos u operativos a otros titulares o usuarios de redes o servicios de comunicaciones electrónicas, podrá adoptar medidas provisionales de urgencia para remediar la situación, entre las que se incluyen la suspensión provisional de la eficacia del título, la orden de cese inmediato del uso del dominio público radioeléctrico, el precintado o la incautación de los equipos o aparatos o la clausura de las instalaciones utilizadas con ocasión del incumplimiento, entre otras.

El titular dispondrá de un plazo de quince días a contar desde que se adopten las medidas provisionales para presentar las alegaciones que estime oportuno y proponer posibles vías de solución.

La Agencia Estatal de Radiocomunicaciones, a la vista de las alegaciones y de las soluciones propuestas por el titular, acordará el levantamiento de las medidas provisionales si se subsana el incumplimiento. En caso contrario, podrá acordar la continuación en la aplicación de las medidas provisionales y propondrá al Ministerio de Industria, Turismo y

Comercio la incoación de un expediente sancionador en los términos indicados en el apartado 3 de este artículo.

Sección 2.ª Procedimiento de licitación

Artículo 29. *Otorgamiento de concesiones para el uso del dominio público radioeléctrico por el procedimiento de licitación.*

1. Cuando sea preciso para garantizar el uso eficaz del dominio público radioeléctrico o cuando la demanda de uso supere a la oferta, el Ministerio de Industria, Turismo y Comercio podrá limitar el número de concesiones a otorgar en determinadas bandas de frecuencias, de acuerdo con lo establecido en los artículos 44.2 y 45.2.b) de la Ley General de Telecomunicaciones.

La Agencia Estatal de Radiocomunicaciones, tras constatar que el número de solicitudes supera la oferta de dominio público radioeléctrico o previa consulta pública para conocer la existencia de posibles interesados en la obtención de derechos de uso sobre determinadas bandas de frecuencias, incluyendo en dicha consulta a las asociaciones de consumidores y usuarios, suspenderá el otorgamiento de los títulos habilitantes correspondientes, proponiendo al Ministerio de Industria, Turismo y Comercio que incluya esas bandas de frecuencias dentro de la relación en la que el número de concesiones a otorgar queda limitado, a efecto de proceder al inicio de un procedimiento de licitación.

2. El procedimiento de licitación no será de aplicación al otorgamiento de los recursos radioeléctricos cuando así lo requiera la aplicación de normas internacionales o convenios que obliguen al Reino de España.

3. Al procedimiento de licitación que, en su caso, se adopte será de aplicación lo siguiente:

a) Mediante orden del Ministerio de Industria, Turismo y Comercio, previo informe preceptivo de la Comisión del Mercado de las Telecomunicaciones, se aprobará el pliego de bases y la convocatoria de un procedimiento de licitación para el otorgamiento de los títulos. En el citado pliego deberá establecerse:

1) La cantidad de dominio público reservada, las características de su utilización, el plazo de vigencia de los títulos o cualquier otra característica o condición para su uso efectivo.

2) El plazo para la presentación de las ofertas, que no podrá ser inferior a un mes.

3) Los requisitos y condiciones que hayan de cumplir los licitadores y los posibles adjudicatarios, que, en su caso, deberán ostentar la condición de operador en el momento de finalización del plazo de presentación de solicitudes.

4) El procedimiento de adjudicación, que podrá ser concurso, subasta o una combinación de ambos, respetando en todo caso los principios de publicidad, concurrencia y no discriminación.

En el caso de que se opte por el concurso como procedimiento de adjudicación, ya sea de manera individualizada o en combinación con la subasta, serán criterios de valoración según la naturaleza del servicio:

a. Los plazos de despliegue de red y de cobertura.

b. Las cantidades a destinar en inversión nueva.

c. El número de estaciones radioeléctricas a desplegar.

d. Las técnicas que permitan hacer un uso más eficaz y eficiente del dominio público radioeléctrico.

La evaluación de estos criterios y la propuesta de adjudicación se efectuará por una Mesa de Adjudicación. La Mesa estará constituida por un Presidente, un mínimo de cinco vocales y un Secretario.

Los miembros de la Mesa serán nombrados por el Ministro de Industria, Turismo y Comercio. El Secretario deberá ser designado entre funcionarios de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, y entre los vocales deberán figurar necesariamente un funcionario de entre quienes tengan atribuido legal o reglamentariamente el asesoramiento jurídico y un interventor.

5) La cuantía de la garantía provisional y la garantía definitiva cuya constitución pueda exigirse en función de la naturaleza de la red o del servicio.

6) Las condiciones en que deba prestarse el servicio o explotarse la red de comunicaciones electrónicas a que esté destinado el dominio público radioeléctrico reservado.

b) En todo lo no previsto en el pliego de bases en relación con la convocatoria, adjudicación, modificación, transmisión, cesión y extinción de los títulos otorgados mediante este procedimiento será de aplicación la legislación del Patrimonio de las Administraciones Públicas.

c) El procedimiento de licitación deberá resolverse mediante orden del Ministro de Industria, Turismo y Comercio y notificarse en un plazo máximo de ocho meses desde la publicación de la convocatoria.

d) Las condiciones en que deba prestarse el servicio o explotarse la red mediante el uso efectivo del dominio público radioeléctrico reservado, serán las previstas en la Ley General de Telecomunicaciones y su normativa de desarrollo, las específicas establecidas en el pliego de bases y las que el licitador, en su caso, haya asumido en su propuesta.

4. La relación de bandas de frecuencia con limitación del número de títulos habilitantes de uso del dominio público radioeléctrico será revisable por el Ministerio de Industria, Turismo y Comercio, de oficio o a instancia de parte, en todo caso cada dos años. En caso de efectuarse dicha revisión, no habrá derecho a indemnización a favor de los titulares que hubieran obtenido sus concesiones mediante el procedimiento de licitación, sin perjuicio del derecho de los mismos a la cancelación de las garantías que, en su caso, hubiesen constituido para responder de compromisos asumidos en el procedimiento.

5. En el caso de concesiones para el uso privativo del dominio público radioeléctrico otorgadas por un procedimiento de licitación, las competencias sobre renovación, modificación, extinción, revocación, cesión y transferencia del título corresponde al Ministro de Industria, Turismo y Comercio.

CAPÍTULO III

Uso privativo del dominio público radioeléctrico para fines especiales

Sección 1.ª De los recursos órbita-espectro

Artículo 30. *Recursos órbita-espectro: Concepto y naturaleza.*

1. Son recursos órbita-espectro, a los efectos de este reglamento, aquellos necesarios para soportar una infraestructura satelital de radiocomunicaciones constituida por cada una de las posiciones de la órbita geoestacionaria o bien un conjunto de órbitas no geoestacionarias susceptibles de albergar un sistema de satélites, las zonas de servicio y las frecuencias espaciales precoordinadas.

2. La utilización de los derechos del Reino de España sobre los recursos órbita-espectro estará sometida al derecho internacional y, en particular, a lo dispuesto en los Tratados de la Constitución, Convenio y Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT). Las relaciones del Reino de España con la UIT para tramitar las reservas de recursos órbita-espectro a favor del Reino de España están excluidas de la regulación de este reglamento, que tiene por objeto las relaciones entre la Administración española y los interesados en la obtención a su favor de los derechos de uso sobre dichos recursos.

3. El derecho de uso de recursos órbita-espectro en el ámbito de la soberanía española tendrá la consideración de derecho de uso privativo de dominio público radioeléctrico y le será de aplicación, además de lo previsto en este capítulo, lo establecido en la Ley General de Telecomunicaciones y sus normas de desarrollo.

Artículo 31. *Títulos habilitantes para el uso privativo de recursos órbita-espectro.*

1. Los derechos de uso de los recursos órbita-espectro se obtendrán mediante concesión o afectación demanial en los términos previstos en este reglamento.

2. Una vez publicada por la UIT la información relativa a la solicitud de reserva de recurso órbita-espectro presentada por el Reino de España, se podrá otorgar una autorización provisional para la explotación de dicho recurso, si se reúnen todas las condiciones requeridas para dicha explotación. En todo caso, dicha autorización estará condicionada a las características técnicas y limitaciones derivadas del proceso de coordinación internacional y podrá ser cancelada si se producen problemas técnicos en la explotación del recurso órbita-espectro o si la UIT no reconoce la reserva del recurso órbita-espectro a favor del Reino de España.

3. Las frecuencias de la red terrenal subordinada a la infraestructura satelital de radiocomunicaciones no se otorgarán incluidas en el título habilitante para el uso privativo del recurso órbita-espectro, siendo necesario el otorgamiento del correspondiente título habilitante para el uso de dicho dominio público radioeléctrico.

Artículo 32. *Otorgamiento de derechos de uso de recursos órbita-espectro mediante afectación demanial.*

1. El otorgamiento de derechos de uso de recursos órbita-espectro a favor de Administraciones Públicas destinados total o principalmente a la prestación por éstas de los servicios que tengan encomendados se realizará mediante afectación demanial.

2. En la utilización de la capacidad excedentaria de los recursos órbita-espectro cuyos derechos de uso hayan sido otorgados mediante afectación con el objetivo de la prestación de servicios a terceros en el mercado, será de aplicación lo dispuesto en el artículo 4 del reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto, 424/2005, de 15 de abril.

3. Los recursos órbita-espectro cuyos derechos de uso hayan sido afectados a una Administración Pública para la atención de los fines para los que fueron solicitados podrán ser utilizados por ésta mediante gestión directa o indirecta, de conformidad con lo establecido en su normativa específica.

Artículo 33. *Procedimiento de otorgamiento de los derechos de uso de recursos órbita-espectro.*

1. A las solicitudes de otorgamiento de título habilitante para el uso privativo de los recursos órbita-espectro les será de aplicación lo establecido en los capítulos I y II del título IV, sin perjuicio de las condiciones específicas enumeradas en este artículo.

2. Los interesados en obtener cualquier título habilitante para el uso privativo de los recursos órbita-espectro presentarán sus solicitudes preferentemente ante la Agencia Estatal de Radiocomunicaciones, o en cualquiera de los lugares previstos en el artículo 38.4 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien a través de los registros telemáticos correspondientes conforme a la normativa vigente.

La solicitud deberá ir acompañada, además de con la documentación administrativa especificada en el apartado a) del artículo 21 de este reglamento, con la siguiente documentación:

a) Memoria técnica en la que se indiquen las características de la red o sistema de satélites, así como de los servicios de comunicaciones por satélite a ofrecer, cobertura prevista, calidad de la señal, balances de los distintos enlaces, entre otros, así como su adecuación a la normativa en vigor y al Reglamento de Radiocomunicaciones de la UIT.

b) Declaración del material, instalaciones y equipo técnico que tenga previsto utilizar en la ejecución del proyecto.

c) Presupuesto económico desglosado y total estimado para la ejecución íntegra del proyecto, incluyendo el segmento espacial y el segmento terreno, así como los costes de lanzamiento y seguros.

d) Compromiso de que los centros de gestión y estaciones de control del sistema de satélites estarán radicados en España.

e) Solvencia económica y técnica, que deberá acreditarse mediante la presentación de los siguientes documentos:

1. Balances o extractos de balances del último ejercicio económico, debidamente auditados.

2. Declaración relativa a la cifra de negocios global en los últimos tres ejercicios.

3. Relación de los principales servicios o trabajos realizados en los últimos tres años que incluya importe, fechas y beneficiarios públicos o privados de los mismos.

4. Declaración que indique el promedio anual de personal y plantilla de directivos durante los tres últimos años.

5. Declaración de las medidas adoptadas por los empresarios para controlar la calidad, así como de los medios de estudio y de investigación de que dispongan.

6. Cualificación de los cuadros técnicos relacionados con el proyecto.

3. El interesado se hará cargo directamente y a su costa de cualquier obligación económica que genere la UIT en relación con el procedimiento de reserva del recurso órbita-espectro.

A tal efecto, en el caso de que el título habilitante solicitado para el uso del recurso órbita-espectro fuera una concesión demanial, la Agencia Estatal de Radiocomunicaciones, antes de dictar la resolución sobre el otorgamiento del mismo, exigirá la constitución por el interesado de una garantía destinada a asegurar el cumplimiento del compromiso de hacer frente a cualquier obligación económica que genere la UIT en relación con el procedimiento de reserva del recurso órbita-espectro.

Como norma general, la cuantía de la garantía a la que hace referencia el párrafo anterior, será de 600.000 euros. No obstante, podrán exigirse garantías inferiores en función de la simplicidad del procedimiento a desarrollar.

La garantía deberá constituirse y depositarse en la Caja General de Depósitos, en los términos establecidos en el Real Decreto 161/1997, de 7 de febrero, que aprueba el Reglamento de la Caja General de Depósitos, en el plazo de un mes a contar desde el requerimiento efectuado al efecto por la Agencia Estatal de Radiocomunicaciones.

4. La Agencia Estatal de Radiocomunicaciones, antes de dictar la resolución sobre el otorgamiento o denegación del título habilitante necesario para el uso del recurso órbita-espectro, podrá requerir al solicitante cuanta información, estudios o aclaraciones considere convenientes sobre su solicitud o sobre los documentos con ella presentados. En concreto, podrá requerir cuantos datos y documentos adicionales considere necesarios para evaluar la solvencia económica y técnica del solicitante, así como la viabilidad del proyecto.

El solicitante está obligado a aportar a su costa a la Agencia Estatal de Radiocomunicaciones la información, estudios o aclaraciones que le haya requerido. En caso de que el solicitante no aporte la información, estudios o aclaraciones requeridos, o bien los mismos sean insuficientes para continuar con el normal desarrollo del procedimiento de reconocimiento por la UIT de la reserva del recurso órbita-espectro y posterior otorgamiento del título habuilitante para el uso de dicho recurso, la Agencia Estatal de Radiocomunicaciones dictará resolución por la que se le tenga por desistido de su solicitud.

5. El plazo de que dispone la Agencia Estatal de Radiocomunicaciones para resolver las solicitudes de otorgamiento de títulos habilitantes para el uso privativo de recursos órbita-espectro será de seis semanas a contar desde que la UIT haya reconocido la reserva del recurso órbita-espectro a favor del Reino de España.

6. La Agencia Estatal de Radiocomunicaciones podrá denegar mediante resolución motivada las solicitudes, además de por alguna de las causas mencionadas en el artículo 23, por las siguientes:

a) Falta de solvencia económica o técnica del solicitante o falta de viabilidad del proyecto.

b) Razones de interés público, de fomento de competencia en los mercados de redes y servicios de comunicaciones electrónicas o de desarrollo del sector de las telecomunicaciones y de la Sociedad de la Información, debidamente acreditadas. En este caso, los daños y perjuicios que se deriven de los gastos en que hubiese incurrido el solicitante con ocasión de la tramitación de su solicitud darán derecho a indemnización.

7. Los títulos habilitantes para el uso privativo del recurso órbita-espectro se otorgarán por un período de tiempo de veinte años.

Artículo 34. *Obligaciones específicas de los titulares de los derechos de uso de recursos órbita-espectro.*

Son obligaciones específicas de los titulares de los derechos de uso de recursos órbita-espectro las siguientes:

a) Cuando a través de dichos recursos órbita-espectro se presten servicios de difusión, el titular de los derechos de uso del recurso órbita-espectro está obligado a notificar a la Agencia Estatal de Radiocomunicaciones y a la Comisión del Mercado de Telecomunicaciones el servicio o servicios concretos que se prestan y el título habilitante de difusión al amparo del cual se proveen los servicios.

b) Impedir el uso del recurso órbita-espectro a los usuarios que carezcan o les haya sido revocado el título para la prestación de servicios de difusión o de comunicaciones electrónicas, según proceda, o que carezcan o les haya sido revocado el título habilitante de derechos de uso de dominio público radioeléctrico para su explotación en redes de comunicaciones electrónicas que utilicen los recursos órbita-espectro a que se refiere la Sección siguiente.

Artículo 35. *Derechos de gratuidad en los procedimientos de obtención de recursos órbita-espectro ante la UIT.*

El Reino de España, como Estado miembro de la UIT, tiene con carácter anual el derecho de gratuidad sobre la unidad más simple de recursos orbitales definida como «red de satélite» por la UIT.

Para la selección de la red susceptible de aplicación del procedimiento de gratuidad, se aplicarán los siguientes criterios conforme al siguiente orden de prelación:

a) Redes de satélite cuyo operador sea una Administración Pública, frente a otras posibles redes.

b) Red que suponga el coste más elevado, siempre que sea compatible con las decisiones del Consejo de la UIT.

Sección 2.ª Uso del dominio público radioeléctrico para su explotación mediante la utilización de recursos órbita-espectro

Artículo 36. *Otorgamiento de derechos de uso privativo del dominio público radioeléctrico para su explotación en redes de comunicaciones electrónicas que utilicen los recursos órbita-espectro.*

1. A las solicitudes de otorgamiento de derechos de uso privativo de dominio público radioeléctrico para su explotación en redes de comunicaciones electrónicas que utilicen satélites les será de aplicación lo establecido en los capítulos I y II del título IV, sin perjuicio de las especialidades enumeradas en este artículo.

2. Los solicitantes de estos derechos de uso deberán acreditar fehacientemente que disponen o están en condiciones de disponer de la capacidad de segmento espacial correspondiente proporcionada por el titular de la infraestructura satelital. La falta de acreditación de este requisito será causa de denegación de la solicitud por la Agencia Estatal de Radiocomunicaciones.

3. El otorgamiento del título habilitante del uso del dominio público radioeléctrico para el acceso a estaciones terrenas de enlace con una estación espacial, cuya titularidad corresponda a una Administración extranjera, o la prestación de servicios basados en la misma requerirá, sin perjuicio de los acuerdos internacionales celebrados por el Estado español, el cumplimiento de las siguientes condiciones:

a) La estación espacial deberá estar inscrita en el Registro Internacional de frecuencias de la UIT.

b) Deberá existir un acuerdo de reciprocidad expreso que reconozca a las personas físicas o jurídicas españolas el derecho a prestar servicios similares en el país del que sea nacional la persona física o jurídica solicitante del título habilitante.

Sección 3.ª Uso del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y televisión

Artículo 37. *Uso del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión.*

1. Al derecho de uso del dominio público radioeléctrico destinado a la prestación de servicios de radiodifusión sonora y televisión a través de redes de satélites le será de aplicación lo dispuesto en las secciones 1.ª y 2.ª de este capítulo.

2. El derecho de uso privativo del dominio público radioeléctrico planificado para la prestación de servicios de televisión digital en movilidad y otros servicios adicionales, cuando no se realice a través de redes de satélite, se otorgará de conformidad con lo previsto en la legislación aplicable y, en su caso, en los planes técnicos nacionales.

3. Para los restantes supuestos de prestación de servicios de radiodifusión sonora y televisión por ondas terrestres, el derecho de uso de dominio público radioeléctrico se otorgará, de conformidad con lo previsto en los planes técnicos nacionales, por la Administración de las Telecomunicaciones mediante concesión demanial aneja a quien disponga del correspondiente título habilitante para la prestación de dichos servicios de difusión.

4. La utilización del dominio público radioeléctrico para redes punto a punto de transporte de señales de los servicios de radiodifusión sonora y de televisión quedan excluidas de lo dispuesto en este artículo y les será de aplicación lo dispuesto en el presente reglamento con carácter general.

Sección 4.ª Uso del dominio público radioeléctrico para fines experimentales y eventos de corta duración

Artículo 38. *Concepto, títulos habilitantes y régimen jurídico.*

1. A los efectos de este reglamento, tendrán la consideración de eventos de corta duración los de cobertura de acontecimientos deportivos, culturales u otros de especial interés. Asimismo, tendrán la consideración de usos experimentales los destinados a efectuar pruebas técnicas o ensayos sobre propagación, utilización de nuevas bandas de frecuencia o demostraciones de nuevos servicios o tecnologías.

2. El uso del dominio público radioeléctrico para eventos de corta duración y para usos experimentales se regirá por lo establecido para las autorizaciones administrativas de uso privativo del dominio publico radioeléctrico, excepto en lo relativo a la duración de las autorizaciones administrativas para eventos de corta duración que será por un máximo de seis meses improrrogables.

3. En las solicitudes de autorización administrativa de uso del dominio público radioeléctrico para eventos de corta duración o con fines experimentales, se podrá sustituir la documentación administrativa a que se refiere el artículo 20 de este reglamento, por una acreditación fehaciente de la personalidad del solicitante, y la propuesta técnica por una descripción de los equipos que se pretenden utilizar, con indicación de sus características técnicas y plazos de utilización.

TÍTULO V

Transferencia de títulos habilitantes y cesión de derechos de uso del dominio público radioeléctrico

CAPÍTULO I

Disposiciones generales

Artículo 39. *Objeto y concepto.*

1. El objeto de este título es la regulación de la transferencia de títulos habilitantes y de la cesión a terceros de los derechos de uso privativo del dominio público radioeléctrico.

2. En la transferencia de títulos habilitantes para el uso privativo del dominio público radioeléctrico se transmite la titularidad, total o parcial, del título habilitante.

3. En la cesión de derechos de uso privativo del dominio público radioeléctrico se transmite el derecho a utilizar determinadas frecuencias vinculadas al título.

4. La transferencia de títulos habilitantes o la cesión de derechos de uso privativo del dominio público radioeléctrico no implica alteración alguna en el ámbito objetivo de los derechos y obligaciones del título originario.

Artículo 40. *Autorización administrativa previa.*

Toda transferencia de títulos habilitantes y toda cesión de derechos de uso privativo del dominio público radioeléctrico debe ser autorizada previamente por el órgano competente para el otorgamiento del título. El negocio jurídico de transferencia o de cesión efectuado que no tenga esa autorización administrativa previa será nulo de pleno derecho y se tendrá por no celebrado.

Artículo 41. *Exclusiones comunes.*

1. No serán susceptibles de transferencia las afectaciones demaniales ni las autorizaciones de uso especial del dominio público radioeléctrico, así como tampoco se podrán ceder los derechos de uso del dominio público radioeléctrico a que habiliten las afectaciones demaniales o las autorizaciones de uso especial.

2. No se pueden transferir los títulos habilitantes ni ceder los derechos de uso del dominio público radioeléctrico relacionados con la seguridad pública y la defensa nacional ni con el cumplimiento de las obligaciones de servicio público a que se refiere el Título III de la Ley General de Telecomunicaciones impuestas en el título original.

3. Igualmente, no se pueden transferir los títulos habilitantes ni ceder los derechos de uso del dominio público radioeléctrico en los que se acredite que supondría una restricción de la competencia en el mercado. En este caso, se solicitará previamente informe a la Comisión del Mercado de las Telecomunicaciones.

4. No serán susceptibles de transferencia los títulos habilitantes ni se podrán ceder los derechos de uso del dominio público radioeléctrico cuando su titular se encuentre incurso en un procedimiento administrativo del que pueda derivarse la revocación del título habilitante.

Artículo 42. *Requisitos.*

1. El titular de los derechos de uso a ceder o del título a transferir deberá encontrarse, a la fecha de autorización de la transmisión, al corriente del cumplimiento de cualquier obligación inherente al título habilitante del que es titular.

En el caso del abono de la tasa por reserva del dominio público radioeléctrico, se entenderá que se está al corriente del cumplimiento de esta obligación cuando, en el procedimiento de impugnación en vía administrativa o contencioso-administrativa interpuesto contra la liquidación de la tasa, se hubiese acordado la suspensión del acto impugnado.

2. El nuevo titular del título o de los derechos de uso deberá reunir las condiciones que, de acuerdo con la Ley General de Telecomunicaciones y su normativa de desarrollo,

resulten exigibles para la explotación de la red o la prestación del servicio al que se pretende destinar los derechos o el título obtenido, así como deberá cumplir todos los requisitos exigidos en el presente reglamento para la obtención del título habilitante.

3. Las condiciones técnicas de uso de los derechos cedidos o de los títulos transferidos se ajustarán, en cualquier caso, a las establecidas en el Cuadro Nacional de Atribución de Frecuencias, en los planes técnicos correspondientes y en este reglamento, así como a las que, en su caso, estén fijadas en acuerdos internacionales, normativa de la Unión Europea y acuerdos de coordinación de frecuencias con otros países.

Asimismo, se deberán respetar las condiciones técnicas de uso que, en su caso, existieran en el título original, como las limitaciones derivadas de servidumbres radioeléctricas, limitaciones por razones de compatibilidad entre servicios, niveles máximos de emisión y protección de los centros de control de emisiones radioeléctricas de la Administración, entre otras.

Artículo 43. *Normas generales del procedimiento administrativo de autorización.*

1. El procedimiento administrativo de autorización de la transferencia de título habiltante o de la cesión a terceros de los derechos de uso privativo del dominio público radioeléctrico se iniciará siempre a instancia de parte interesada.

2. La solicitud, que deberá ir firmada conjuntamente por el nuevo y el anterior titular, con indicación del domicilio a efectos de notificaciones, se presentará ante el órgano competente para el otorgamiento del título o en cualquiera de los lugares previstos en el artículo 38.4 de la Ley, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien, a través de los registros telemáticos correspondientes conforme a la normativa vigente.

La solicitud deberá ir acompañada de la siguiente documentación:

a) Copia del negocio jurídico a suscribir entre los titulares.

b) Datos identificativos del nuevo y del anterior titular y, en su caso, de las personas que los representen, incluyendo nombre o razón social.

c) Referencia del título habilitante afectado por el negocio jurídico.

d) Fecha de inicio del negocio jurídico, y, en el caso de cesión, su fecha de finalización.

e) Documentos que acrediten la condición de operador de comunicaciones electrónicas del nuevo titular.

f) Porción de dominio público radioeléctrico objeto del negocio jurídico y zona geográfica de utilización.

g) Características técnicas de las redes y servicios en los que se prevé utilizar los derechos de uso del dominio público objeto del negocio jurídico.

h) Declaración del anterior titular de haber comunicado al nuevo titular las condiciones técnicas de uso del dominio público radioeléctrico objeto del negocio jurídico.

i) Declaración del nuevo titular de que conoce y asume la responsabilidad en el uso del dominio público radioeléctrico objeto del negocio jurídico, incluyendo los aspectos técnicos tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

Artículo 44. *Revocación de la autorización.*

El órgano administrativo que dictó la autorización administrativa previa de la transferencia de título habilitante o de cesión de derechos de uso de dominio público radioeléctrico podrá acordar, mediante resolución motivada, su revocación y, en consecuencia, la extinción del negocio jurídico autorizado, por las siguientes causas:

a) El incumplimiento de las condiciones esenciales de la transmisión en los términos en que fue autorizada.

b) La existencia de interferencias perjudiciales o incompatibilidades electromagnéticas que degraden la calidad de los servicios prestados u otros previamente autorizados, originados como consecuencia de la transmisión.

c) La revocación del título habilitante original en el caso de las cesiones de derechos de uso del dominio público radioeléctrico.

CAPÍTULO II

Transferencia de títulos que habilitan al uso del dominio público radioeléctrico

Artículo 45. *Concepto.*

En la transferencia de títulos habilitantes para el uso privativo del dominio público radioeléctrico se transmite la titularidad, total o parcial, del título habilitante.

Artículo 46. *Subrogación de derechos.*

El nuevo titular se subrogará en todos los derechos y obligaciones del anterior titular derivados del título transferido. En particular, en el caso de las concesiones demaniales otorgadas por el procedimiento de licitación, el nuevo titular se subrogará en todas las condiciones especificadas en el pliego de bases por el que se rigió dicho procedimiento, así como en todos los compromisos asumidos por el anterior titular en la oferta que sirvió de base para la adjudicación.

Artículo 47. *Modalidades de transferencia.*

La transferencia de títulos habilitantes para el uso privativo del dominio público radioeléctrico puede revestir alguna de las dos siguientes modalidades:

a) Transferencia total.

b) Transferencia parcial.

Artículo 48. *Transferencia total.*

1. La transferencia total de títulos habilitantes para el uso privativo del dominio público radioeléctrico es aquella en que se transmite la titularidad del título habilitante en su totalidad y, en consecuencia, se transmite la totalidad de los derechos de uso privativo del dominio público radioeléctrico derivados del título, por todo el período de tiempo que reste de vigencia y en todo el ámbito geográfico del título.

2. La transferencia total de títulos habilitantes para el uso privativo del dominio público radioeléctrico podrá ser autorizada con independencia de la banda de frecuencias afectada.

Artículo 49. *Transferencia parcial.*

1. La transferencia parcial de títulos habilitantes para el uso privativo del dominio público radioeléctrico es aquélla en la que se transmite la titularidad de una parte del título, ya sea porque se transmite la titularidad de una parte de los derechos de uso en relación con la utilización de las frecuencias otorgadas en un área geográfica determinada que forme parte del ámbito geográfico sobre el que el título original otorgó los derechos de uso del dominio público radioeléctrico, ya sea porque se transmite la titularidad de una parte de las frecuencias o bandas de frecuencias otorgadas.

2. Sólo son susceptibles de transferencia parcial de títulos habilitantes aquéllos en los que la parte de los derechos de uso privativo del dominio público radioeléctrico que se transmite son atribuidos a los servicios con frecuencias reservadas en las bandas a las que hace referencia el anexo de este reglamento.

Artículo 50. *Autorización de la transferencia.*

1. El órgano competente para el otorgamiento del título, previo análisis de la solicitud y de la documentación aportada, así como de las condiciones que figuren en el negocio jurídico a celebrar entre las partes interesadas, y recabando, en su caso, los informes de cualesquiera otros órganos de la Administración que se consideren pertinentes, dictará resolución motivada autorizando o denegando la celebración del negocio jurídico.

2. El plazo para resolver la solicitud será de tres meses, transcurrido el cual sin que haya recaído resolución expresa se entenderá denegada la solicitud, sin perjuicio de la obligación del órgano competente para el otorgamiento del título de resolver expresamente de acuerdo

con lo dispuesto en el artículo 43 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. En el caso de que se autorice la celebración del negocio jurídico y una vez que las partes interesadas remitan copia fehaciente del negocio jurídico suscrito entre los mismos en los términos en los que ha sido autorizado, el órgano competente para el otorgamiento del título dictará una resolución extintiva o modificativa del título original, según sea una transferencia total o parcial del título respectivamente, y otra resolución constitutiva del título habilitante en favor del nuevo titular.

4. El otorgamiento, modificación y extinción de los títulos habilitantes como consecuencia de la celebración autorizada del negocio juridico de la transferencia de títulos habilitantes del uso privativo del dominio público radioeléctrico se inscribirán en el Registro público de concesionarios.

Artículo 51. *Derechos y obligaciones específicos en la transferencia parcial.*

1. El nuevo titular se subrogará en todos los derechos y obligaciones del anterior titular derivados del título transferido en la parte que le corresponda en función del ámbito geográfico o de la parte de las frecuencias o bandas de frecuencias objeto de la transferencia.

En tal sentido, el anterior y el nuevo titular, en documento adicional que deben acompañar a la solicitud de autorización de transferencia, identificarán de manera clara y precisa los derechos y obligaciones que les corresponderá a cada uno de ellos una vez celebrado el negocio jurídico.

2. Ambos titulares podrán solicitar individualmente la renovación de la vigencia de los correspondientes títulos, de acuerdo con lo establecido en este reglamento.

3. Ambos titulares estarán obligados al pago de la correspondiente tasa por reserva del dominio público radioeléctrico en la parte que les corresponda en función de los derechos de uso del dominio público radioeléctrico de los que sean titulares.

Artículo 52. *Transferencias sucesivas.*

Los títulos habilitantes para el uso privativo del dominio público radioeléctrico que hayan sido transferidos podrán ser objeto de nuevas transferencias.

No obstante lo anterior, si los títulos habilitantes se otorgaron mediante un procedimiento de licitación y en el pliego de bases regulador del mismo se fijó un período mínimo en el que el título habilitante no podía ser objeto de transferencia, ésta no podrá efectuarse hasta que transcurra dicho período.

CAPÍTULO III

Cesión de derechos de uso del dominio público radioeléctrico

Artículo 53. *Concepto.*

En la cesión de derechos de uso privativo del dominio público radioeléctrico se transmite el derecho a utilizar determinadas frecuencias vinculadas al título.

Artículo 54. *Ámbito objetivo de la cesión de derechos de uso.*

1. Son susceptibles de cesión los derechos de uso privativo del dominio público radioeléctrico atribuidos a los servicios con frecuencias reservadas en las bandas a las que hace referencia el anexo de este reglamento.

2. La cesión sólo podrá efectuarse sobre los excedentes de capacidad de los derechos de uso del dominio público radioeléctrico de los que se sea titular, entendiendo por tal la parte del dominio público no necesaria para el cumplimiento por el cedente de las obligaciones asumidas frente a la Administración.

3. No se pueden ceder todos los derechos de uso privativo del dominio público radioeléctrico, por todo el período de tiempo y en todo el ámbito geográfico del título del que derivan los derechos, sin perjuicio de que se pueda acordar la transferencia del título de acuerdo con lo dispuesto en los Capítulos I y II de este Título.

4. La cesión podrá ser sobre parte de los derechos de uso del cedente en relación con la utilización de las frecuencias otorgadas en un área geográfica determinada que forme parte del ámbito geográfico sobre el que el título original otorgó los derechos de uso del dominio público radioeléctrico, o por una parte de las frecuencias o bandas de frecuencias otorgadas.

Artículo 55. *Modalidades de cesión.*

La cesión de derechos de uso privativo del dominio público radioeléctrico puede revistir alguna de las dos siguientes modalidades:

a) Cesión por períodos superiores a seis meses.

b) Cesión por períodos de hasta seis meses.

Artículo 56. *Autorización de la cesión por períodos superiores a seis meses.*

1. El órgano competente para el otorgamiento del título, previo análisis de la solicitud y de la documentación aportada, así como de las condiciones que figuren en el negocio jurídico a celebrar entre las partes interesadas, y recabando, en su caso, los informes de cualesquiera otros órganos de la Administración que se consideren pertinentes, dictará resolución motivada autorizando o denegando la celebración del negocio jurídico.

2. El plazo para resolver la solicitud será de tres meses, transcurrido el cual sin que haya recaído resolución expresa se entenderá denegada la solicitud, sin perjuicio de la obligación del órgano competente para el otorgamiento del título de resolver expresamente de acuerdo con lo dispuesto en el artículo 43 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. En el caso de que se autorice la celebración del negocio jurídico y una vez que las partes interesadas remitan copia fehaciente del negocio jurídico suscrito entre los mismos en los términos en los que ha sido autorizado, el órgano competente para el otorgamiento del título se lo comunicará al Registro público de concesionarios.

4. En el caso de que el negocio jurídico de cesión se extinga por cualquier causa con anterioridad a que expire el período de tiempo de vigencia por el que fue suscrito, las partes interesadas tienen la obligación de comunicar dicha circunstancia al órgano competente para el otorgamiento del título y al Registro público de concesionarios.

Artículo 57. *Autorización de la cesión por periodos de hasta seis meses.*

1. El órgano competente para el otorgamiento del título, previo análisis de la solicitud y de la documentación aportada, así como de las condiciones que figuren en el negocio jurídico a celebrar entre las partes interesadas, y recabando, en su caso, los informes de cualesquiera otros órganos de la Administración que se consideren pertinentes, dictará resolución motivada autorizando o denegando la celebración del negocio jurídico.

2. El plazo para resolver la solicitud será de un mes, transcurrido el cual sin que haya recaído resolución expresa se entenderá otorgada la autorización.

Artículo 58. *Derechos y obligaciones específicos en la cesión.*

1. La cesión de los derechos de uso privativo del dominio público radioeléctrico no eximirá al titular del derecho de uso cedente de las obligaciones asumidas frente a la Administración.

2. El cedente se mantendrá como único interlocutor ante la Administración a efectos de posibles modificaciones del título habilitante original o de cualquier otro trámite relacionado con el mismo, incluyendo la obligación del abono de la tasa por reserva de dominio público radioeléctrico por la totalidad de los derechos de uso cedidos.

3. Una vez que la cesión ha concluido en su vigencia, el cedente recuperará automáticamente el uso y disfrute pleno de los derechos de uso cedidos.

Artículo 59. *Cesiones sucesivas.*

Los derechos de uso privativo del dominio público radioeléctrico que hayan sido cedidos no podrán ser objeto de nuevas cesiones sucesivas y simultáneas en el tiempo.

Disposición adicional primera. *Bandas de frecuencias con limitación de títulos habilitantes a otorgar.*

De conformidad con lo previsto en el artículo 29, y sin perjuicio de su modificación por el Ministerio de Industria, Turismo y Comercio, previo informe preceptivo de la Comisión del Mercado de las Telecomunicaciones y previo acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos, la relación de bandas de frecuencias en las que, por ser precisa la garantía del uso eficaz y eficiente del dominio público radioeléctrico, se limita el número de concesiones para su uso es, inicialmente, la siguiente:

a) 790aa 862 MHz.
b) 880 a 915 y 925 a 960 MHz.
c) 1.710 a 1.785 y 1.805 a 1.880 MHz para redes terrestres.
d) 1.900 a 2.025 y 2.110 a 2.200 MHz.
e) 2.500 a 2.690 MHz.
f) 3,4 a 3,6 GHz.

Disposición adicional segunda. *Transformación de los títulos habilitantes para el ejercicio del derecho de uso privativo del dominio público radioeléctrico con limitación de número.*

De acuerdo con lo establecido en el apartado 8, letra d), de la disposición transitoria primera de la Ley General de Telecomunicaciones, los títulos habilitantes para el ejercicio del derecho de uso privativo de dominio público radioeléctrico con limitación de número deben ser transformados en una concesión demanial en los términos y condiciones siguientes:

a) Las resoluciones expresas transformando los títulos existentes con anterioridad a la entrada en vigor de la Ley General de Telecomunicaciones deberán dictarse por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información en el plazo de un año desde la entrada en vigor del presente reglamento. En dichas resoluciones se declarará la anulación del título habilitante actualmente en vigor y su transformación en una concesión de dominio público radioeléctrico independiente de la habilitación de la persona titular de la citada concesión demanial para la prestación del servicio o la explotación de la red de comunicaciones electrónicas.

b) El procedimiento de transformación se iniciará de oficio por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

En el expediente de transformación del título se dará audiencia al titular del mismo, al resto de operadores que tengan asignados derechos de uso privativo de dominio público radioeléctrico dentro de las categorías concretas de títulos habilitantes objeto de transformación a que se refiere el apartado d) de esta disposición, así como a las asociaciones de usuarios.

También se solicitará preceptivamente informe del Servicio Jurídico del Departamento y de la Comisión del Mercado de las Telecomunicaciones, así como dictamen del Consejo de Estado.

Una vez dictada la resolución de transformación, y sin perjuicio de su notificación a los interesados, se dará traslado para conocimiento a la Comisión del Mercado de las Telecomunicaciones.

c) En las resoluciones expresas por las que se transforman los títulos se establecerán los derechos y obligaciones que se declaran subsistentes de los actualmente previstos en los correspondientes títulos. También podrán incluirse otras obligaciones por razones de servicio público e interés general, así como las que se consideren necesarias para preservar las condiciones de competencia en el mercado.

Asimismo, en las condiciones generales y específicas que se establezcan, se tendrán en cuenta las que resulten necesarias para su adecuación al presente reglamento, al Cuadro Nacional de Atribución de Frecuencias y a la normativa de la Unión Europea que, en su caso, resulte de aplicación, en especial, la referida a los principios de neutralidad tecnológica y de los servicios. Dichas condiciones deberán ser, en todo caso, proporcionadas, transparentes y no discriminatorias, La transformación del título no dará derecho a indemnización alguna. En todo caso, se mantendrá el plazo de vigencia para el cual fueron otorgados.

d) Los títulos habilitantes para el ejercicio del derecho de uso privativo de dominio público radioeléctrico con limitación de número objeto de transformación son las concesiones procedentes de las extintas:

i. Licencias individuales de tipo C2 para el establecimiento y explotación de redes públicas fijas de acceso radio en la banda de 26 GHz.

ii. Licencias individuales de tipo C2 para el establecimiento y explotación de redes públicas fijas de acceso radio en la banda de 3,4 a 3,6 GHz.

iii. Licencias individuales de tipo B2 para el establecimiento de la red de telecomunicaciones necesaria y para la explotación del servicio de comunicaciones móviles de tercera generación.

iv. Licencias individuales de tipo B2 para la prestación del servicio de telecomunicación de valor añadido de telefonía móvil automática en su modalidad GSM.

v. Concesiones para la prestación pública del servicio de radiocomunicaciones móviles terrestres en grupos cerrados de usuarios.

vi. Concesiones para la prestación del servicio de telecomunicación de valor añadido de radiocomunicaciones móviles terrestres en grupos cerrados de usuarios.

vii. Licencias individuales de tipo B2 para la prestación del servicio de comunicaciones móviles personales en su modalidad DCS 1800.

Disposición adicional tercera. *Aplicación del principio de neutralidad tecnológica y de servicios.*

En las bandas de frecuencias de 800 MHz, 900 MHz, 1.800 MHz y 2,6 GHz se autoriza la prestación de servicios de comunicaciones electrónicas bajo el principio de neutralidad de servicios.

Disposición adicional cuarta. *Ampliación de las bandas de frecuencia en las que se puede efectuar la transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico.*

1. En las bandas de frecuencias de 800 MHz, 900 MHz, 1.800 MHz, 2.100 MHz, 2,6 GHz y 3,5 GHz se podrán efectuar operaciones de transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico en los términos y con los requisitos establecidos en el Título V del Reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones en lo relativo al uso del dominio público radioeléctrico.

2. La transferencia de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico en estas bandas de frecuencias deberá desarrollarse mediante procedimientos abiertos, transparentes, objetivos y no discriminatorios, y no podrá dar lugar a situaciones anticompetitivas.

ANEXO

Servicios con frecuencias reservadas en las bandas indicadas susceptibles de transferencia parcial de título o de cesión a terceros de los derechos de uso del dominio público radioeléctrico

Servicios	Bandas
Servicios disponibles al público de radiobúsqueda y radiomensajería (Paging).	68 - 87,5 MHz 146 - 174 MHz 406,1 - 430 MHz 440 - 470 MHz
Comunicaciones móviles en grupo cerrado de usuarios.	68 - 87,5 MHz 146 -174 MHz 223 - 235 MHz 410 - 430 MHz 440 - 470 MHz 870 - 876 / 915 - 921 MHz
Servicios de acceso radio disponibles al público.	24,5 - 26,5 GHz

Servicios	Bandas
Servicio fijo punto a punto.	1.427 - 1.452 / 1.492 - 1.518 MHz 1.525 - 1.530 MHz 2.025 - 2.110 / 2.200 - 2.290 MHz 2.290 - 2.300 MHz 3.600 - 4.200 MHz 4.500 - 5.000 MHz 5,9 - 6,4 / 6,4 - 7,1 GHz 7,725 - 7,975 GHz / 8,025 - 8,275 GHz 10,449 - 10,680 GHz 12,75 -13,25 GHz 14,47 - 14,753 / 14,865 - 15,173 GHz 15,285 - 15,350 GHz 17,7 - 19,7 GHz 21,2 - 21,4 GHz 22,0 - 22,6 / 23,0 - 23,6 GHz 27,9405 - 28,4445 / 28,9485 -29,4525 GHz 27,8285 - 27,9405 GHz 31,0 - 31,3 GHz 37,0 - 39,5 GHz

§ 35

Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas

Ministerio de la Presidencia
«BOE» núm. 234, de 29 de septiembre de 2001
Última modificación: 29 de abril de 2005
Referencia: BOE-A-2001-18256

Desde la introducción de manera generalizada de los servicios de radiodifusión de televisión y de radio, hace ya varias décadas, los ciudadanos han disfrutado en su vida cotidiana de los mismos, pero también se han visto sometidos inevitablemente a la exposición de campos electromagnéticos.

La introducción reciente de la competencia en el sector de las telecomunicaciones en España, se ha traducido en una mayor diversidad en la oferta de servicios de telecomunicaciones para empresas y ciudadanos, siendo esto particularmente apreciable en los servicios de telefonía móvil. Esta mayor diversidad de oferta de servicios de telecomunicaciones, y sus niveles de calidad y cobertura asociados, requiere la existencia de un elevado número de instalaciones radioeléctricas.

El Reglamento que se aprueba por este Real Decreto tiene, entre otros objetivos, adoptar medidas de protección sanitaria de la población. Para ello, se establecen unos límites de exposición del público en general a campos electromagnéticos procedentes de emisiones radioeléctricas, acordes con las recomendaciones europeas. Para garantizar esta protección se establecen unas restricciones básicas y unos niveles de referencia que deberán cumplir las instalaciones afectadas por este Real Decreto. Al mismo tiempo, se da respuesta a la preocupación expresada por algunas asociaciones, ciudadanos, corporaciones locales y Comunidades Autónomas.

El presente Real Decreto cumple con las propuestas contenidas en las mociones del Congreso de los Diputados y del Senado, que instaron al Gobierno a desarrollar una regulación relativa a la exposición del público en general a las emisiones radioeléctricas de las antenas de telefonía móvil.

Por otra parte, resulta también necesario, el establecimiento de condiciones que faciliten y hagan compatible un funcionamiento simultáneo y ordenado de las diversas instalaciones radioeléctricas y los servicios a los que dan soporte, considerándose, en particular, determinadas instalaciones susceptibles de ser protegidas.

El artículo 61 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones establece que la gestión del dominio público radioeléctrico y las facultades para su administración y control corresponden al Estado. Además, este artículo añade que dicha gestión se ejercerá atendiendo a la normativa aplicable en la Unión Europea, y a las

resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales.

El artículo 62 de la Ley 11/1998, establece, por su parte, que el Gobierno desarrollará reglamentariamente las condiciones de gestión del dominio público radioeléctrico, precisándose que en dicho Reglamento deberá incluirse el procedimiento de determinación de los niveles de emisión radioeléctrica tolerables y que no supongan un peligro para la salud pública.

El artículo 64, apartado 2, de la Ley 11/1998, dispone que se establecerán reglamentariamente, las limitaciones a la propiedad y las servidumbres, necesarias para la defensa del dominio público radioeléctrico, y para la protección radioeléctrica de las instalaciones de la Administración que se precisen para el control de la utilización del espectro.

El artículo 76 de la Ley 11/1998, establece que es competencia del Ministerio de Fomento (ahora, del Ministerio de Ciencia y Tecnología) la inspección de los servicios y de las redes de telecomunicaciones, de sus condiciones de prestación, de los equipos, de los aparatos, de las instalaciones y de los sistemas civiles, así como la aplicación del régimen sancionador, salvo que corresponda a la Comisión del Mercado de las Telecomunicaciones.

Adicionalmente, el Real Decreto 1451/2000, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Ciencia y Tecnología, atribuye a la Dirección General de Telecomunicaciones y Tecnologías de la Información la competencia para la propuesta de planificación, gestión y administración del dominio público radioeléctrico, para la comprobación técnica de emisiones radioeléctricas, y para el control y la inspección de las telecomunicaciones, así como la aplicación del régimen sancionador en la materia.

La Ley 14/1986, de 25 de abril, General de Sanidad en sus artículos 18, 19, 24 y 40 atribuye a la administración sanitaria las competencias de control sanitario de los productos, elementos o formas de energía que puedan suponer un riesgo para la salud humana. Así mismo, atribuye la capacidad para establecer las limitaciones, métodos de análisis y requisitos técnicos para el control sanitario.

El Real Decreto 1450/2000, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad y Consumo atribuye a la Dirección General de Salud Pública y Consumo la competencia para la evaluación, prevención y control sanitario de las radiaciones no ionizantes.

Para conseguir la protección efectiva de la salud pública es necesario coordinar las competencias del Ministerio de Ciencia y Tecnología, en relación con los límites de emisiones y gestión y protección del dominio público radioeléctrico, con las competencias sanitarias del Ministerio de Sanidad y Consumo.

Asimismo, resulta necesario que ambos Ministerios, con el fin de mejorar los conocimientos que se tienen acerca de la salud y las emisiones radioeléctricas promuevan y revisen la investigación pertinente sobre emisiones radioeléctricas y salud humana, en el contexto de sus programas de investigación nacionales, teniendo en cuenta las recomendaciones comunitarias e internacionales en materia de investigación y los esfuerzos realizados en este ámbito, basándose en el mayor número posible de fuentes.

El Reglamento que se aprueba por este Real Decreto, elaborado en coordinación por los Ministerios de Ciencia y Tecnología y de Sanidad y Consumo, tiene por objeto cumplir con lo establecido en los citados artículos de la Ley 11/1998, sobre emisiones radioeléctricas. Asimismo, el capítulo II, artículos 6 y 7, establece, con carácter de norma básica y en desarrollo de la Ley 14/1986, límites de exposición y condiciones de evaluación sanitaria de riesgos por emisiones radioeléctricas.

El presente Real Decreto asume los criterios de protección sanitaria frente a campos electromagnéticos procedentes de emisiones radioeléctricas establecidos en la Recomendación del Consejo de Ministros de Sanidad de la Unión Europea, de 12 de julio de 1999, relativa a la exposición del público en general a campos electromagnéticos.

Asimismo, esta Recomendación contempla la conveniencia de proporcionar a los ciudadanos información en un formato adecuado sobre los efectos de los campos electromagnéticos y sobre las medidas adoptadas para hacerles frente, al objeto de que se comprendan mejor los riesgos y la protección sanitaria contra la exposición a los mismos.

Este Reglamento establece unos límites de exposición, referidos a los sistemas de radiocomunicaciones, basados en la citada Recomendación del Consejo de la Unión Europea. Además, el Reglamento prevé mecanismos de seguimiento de los niveles de exposición, mediante la presentación de certificaciones e informes por parte de operadores de telecomunicaciones, la realización planes de inspección y la elaboración de un informe anual por parte del Ministerio de Ciencia y Tecnología.

El presente Real Decreto ha sido sometido a audiencia a través del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, y al informe de la Comisión del Mercado de las Telecomunicaciones, de acuerdo con lo previsto en el artículo 1, dos, 2, j) de la Ley 12/1997, de 24 de abril, de Liberalización de las Telecomunicaciones.

El presente Real Decreto ha sido sometido al procedimiento de información en materia de normas y reglamentaciones técnicas y de reglamentos relativos a los servicios de la Sociedad de la Información, previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, de 20 de julio, así como a lo previsto en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información, que incorpora estas Directivas al ordenamiento jurídico español.

En su virtud, a propuesta conjunta de las Ministras de Ciencia y Tecnología y de Sanidad y Consumo, previa aprobación del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 28 de septiembre de 2001,

D I S P O N G O :

Artículo único. *Objeto.*

Mediante el presente Real Decreto se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, que se incluye a continuación con los anexos que lo completan.

DISPOSICIÓN ADICIONAL

Unica. *Elaboración de informes.*

Siguiendo la Recomendación 1999/519/CE del Consejo, de 12 de julio, relativa a la exposición del público en general a campos electromagnéticos, el Ministerio de Sanidad y Consumo elaborará, a los tres años de entrada en vigor de este Reglamento, un informe sobre las experiencias obtenidas en la aplicación del mismo, en lo referido a la protección frente a riesgos sanitarios potenciales de la exposición a las emisiones radioeléctricas.

DISPOSICIÓN DEROGATORIA

Unica. *Derogación normativa.*

Se deroga el capítulo II del título II del Reglamento de desarrollo de la Ley 31/1987, de 18 de diciembre, de Ordenación de las Telecomunicaciones, en relación con el dominio público radioeléctrico y los servicios de valor añadido que utilicen dicho dominio, aprobado por Real Decreto 844/1989, de 7 de julio.

DISPOSICIONES FINALES

Primera. *Desarrollo normativo y modificación de anexos.*

La Ministra de Ciencia y Tecnología dictará las disposiciones necesarias para el desarrollo y aplicación de este Real Decreto. Asimismo, se autoriza a la Ministra de Ciencia y

Tecnología a modificar el anexo I del Reglamento, en función de la experiencia obtenida en su aplicación y de nuevas necesidades.

La Ministra de Sanidad y Consumo dictará las disposiciones necesarias para el desarrollo y aplicación de las funciones atribuidas al Ministerio de Sanidad y Consumo en este Real Decreto. Asimismo, se autoriza a la Ministra de Sanidad y Consumo a modificar el anexo II del Reglamento, de acuerdo con lo establecido en su artículo 7.

Segunda. *Fundamento legal y constitucional.*

Este Real Decreto se dicta en desarrollo de los artículos 48, 62 y 64 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, dictada al amparo del artículo 149.1.21.ª de la Constitución, salvo la disposición adicional única y el capítulo II del Reglamento, artículos 6 y 7, que se dictan en desarrollo de los artículos 18, 19, 24 y 40 de la Ley 14/1986, de 25 de abril, General de Sanidad, con carácter de norma básica, en virtud del artículo 149.1.16.ª de la Constitución.

Tercera. *Entrada en vigor.*

Este Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO QUE ESTABLECE CONDICIONES DE PROTECCIÓN DEL DOMINIO PÚBLICO RADIOELÉCTRICO, RESTRICCIONES A LAS EMISIONES RADIOELÉCTRICAS Y MEDIDAS DE PROTECCIÓN SANITARIA FRENTE A EMISIONES RADIOELÉCTRICAS

CAPITULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente Reglamento tiene por objeto el desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al establecimiento de condiciones de protección del dominio público radioeléctrico, a la autorización, planificación e inspección de instalaciones radioeléctricas en relación con los límites de exposición a las emisiones, el establecimiento de otras restricciones a las emisiones radioeléctricas, la evaluación de equipos y aparatos y el régimen sancionador aplicable. Asimismo, se desarrolla la Ley 14/1986, de 25 de abril, General de Sanidad, en relación con el establecimiento de límites de exposición para la protección sanitaria y la evaluación de riesgos por emisiones radioeléctricas.

Artículo 2. *Ámbito de aplicación.*

Las disposiciones de este Reglamento se aplican a las emisiones de energía en forma de ondas electromagnéticas, que se propagan por el espacio sin guía artificial, y que sean producidas por estaciones radioeléctricas de radiocomunicaciones o recibidas por estaciones del servicio de radioastronomía.

A los efectos de lo dispuesto en el párrafo anterior, se considera estación radioeléctrica uno o más transmisores o receptores, o una combinación de ambos, incluyendo las instalaciones accesorias, o necesarias para asegurar un servicio de radiocomunicación o el servicio de radioastronomía.

CAPITULO II

Protección del dominio público radioeléctrico

Artículo 3. *Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

1. De conformidad con lo establecido en el artículo 48.2 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, podrán imponerse las limitaciones a la propiedad y a la intensidad de campo eléctrico y las servidumbres que resulten necesarias para la adecuada protección radioeléctrica de las instalaciones siguientes:

a) Las instalaciones de la Administración que se precisen para el control de la utilización del espectro radioeléctrico.
b) Las estaciones de socorro y seguridad.
c) Las instalaciones de interés para la defensa nacional.
d) Las estaciones terrenas de seguimiento y control de satélites.
e) Las estaciones de investigación espacial, de exploración de la Tierra por satélite, de radioastronomía y de astrofísica, y las instalaciones oficiales de investigación o ensayo de radiocomunicaciones u otras en las que se lleven a cabo funciones análogas.
f) Cualquier otra instalación o estación cuya protección resulte necesaria para el buen funcionamiento de un servicio público, incluidos los supuestos previstos en el artículo 51 del Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, aprobado por el Real Decreto 1736/1998, de 31 de julio, o en virtud de acuerdos internacionales.

2. Los valores máximos de las limitaciones y servidumbres que resulten necesarias para la protección radioeléctrica de las instalaciones a que se refiere este artículo figuran en el anexo I de este Reglamento.
3. Las servidumbres y limitaciones aeronáuticas se regirán por su normativa específica.
4. El presente Reglamento será de aplicación supletoria en los supuestos regulados en el Reglamento de la Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional, aprobado por el Real Decreto 689/1978, de 10 de febrero.

Artículo 4. *Concepto de limitaciones a la propiedad y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

1. A efectos de lo dispuesto en el presente capítulo, se entenderá por limitación a la propiedad para la protección radioeléctrica de instalaciones, la obligación de no hacer y de soportar no individualizada, impuesta a los titulares y propietarios de los predios cercanos a las estaciones o instalaciones objeto de la protección.

Asimismo, de acuerdo con el artículo 48 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, se entenderá por servidumbre la obligación de no hacer y de soportar de carácter individualizado, indemnizable en los términos de la legislación de expropiación forzosa. Igualmente, las limitaciones a la propiedad, cuando efectivamente causen una privación singular, serán indemnizables con arreglo a lo dispuesto en la legislación sobre expropiación forzosa.

2. Los propietarios no podrán realizar obras o modificaciones en los predios sirvientes que impidan dichas servidumbres o limitaciones, una vez que las mismas se hayan constituido, según lo previsto en el artículo 5 de este Reglamento.

La constitución de dichas servidumbres y limitaciones deberá reducir en lo posible el gravamen que las mismas impliquen y someterse a las reglas de congruencia y proporcionalidad.

Artículo 5. *Constitución de limitaciones y servidumbres.*

1. Los expedientes de constitución de las limitaciones que no causen una privación singular, se iniciarán por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, de oficio o a instancia de parte, y contendrán, como mínimo, la motivación de su necesidad, su ámbito geográfico y su alcance.

2. Dichos expedientes se someterán a las reglas de publicidad, de igualdad de trato y de generalidad de la limitación y se someterán al trámite de audiencia previsto en el artículo 84 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. No obstante, se podrá omitir este trámite de audiencia en ausencia de interesados conocidos. En todo caso, se publicará un extracto en el «Boletín Oficial del Estado» para información pública, otorgándose un plazo de veinte días para la presentación de alegaciones.

3. Concluida la tramitación del expediente administrativo, la Ministra de Ciencia y Tecnología, a propuesta de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, y previo informe de la Abogacía del Estado en el Departamento, resolverá sobre dicho expediente.

4. La Orden de aprobación de la limitación se publicará en el «Boletín Oficial del Estado» y se notificará a los interesados en los términos previstos en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

5. Los expedientes para la constitución de las servidumbres y de las limitaciones que efectivamente causen una privación singular, se iniciarán por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, de oficio o a instancia de parte, y se regirán por lo dispuesto en la legislación sobre expropiación forzosa.

CAPITULO III

Límites de exposición para la protección sanitaria y evaluación de riesgos por emisiones radioeléctricas

Artículo 6. *Límites de exposición a las emisiones radioeléctricas. Restricciones básicas y niveles de referencia.*

En cumplimiento de lo dispuesto en el artículo 62 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y en desarrollo de la Ley 14/1986, de 25 de abril, General de Sanidad, de acuerdo con la Recomendación del Consejo de Ministros de Sanidad de la Unión Europea, de 12 de julio de 1999, y con el fin de garantizar la adecuada protección de la salud del público en general, se aplicarán los límites de exposición que figuran en el anexo II.

Los límites establecidos se cumplirán en las zonas en las que puedan permanecer habitualmente las personas y en la exposición a las emisiones de los equipos terminales, sin perjuicio de lo dispuesto en otras disposiciones específicas en el ámbito laboral.

Artículo 7. *Evaluación sanitaria de riesgos por emisiones radioeléctricas.*

En función de la evidencia científica disponible y de la información facilitada por el Ministerio de Ciencia y Tecnología, el Ministerio de Sanidad y Consumo, en coordinación con las Comunidades Autónomas, evaluará los riesgos sanitarios potenciales de la exposición del público en general a las emisiones radioeléctricas.

En la evaluación se tendrán en consideración el número de personas expuestas, sus características epidemiológicas, edad, partes del organismo expuestas, tiempo de exposición, condiciones sanitarias de las personas y otras variables que sean relevantes para la evaluación.

El Ministerio de Sanidad y Consumo, en coordinación con las Comunidades Autónomas, desarrollará los criterios sanitarios destinados a evaluar las fuentes y prácticas que puedan dar lugar a la exposición a emisiones radioeléctricas de la población, con el fin de aplicar

medidas para controlar, reducir o evitar esta exposición. La aplicación de estas medidas se realizará en coordinación con el Ministerio de Ciencia y Tecnología.

Asimismo, el Ministerio de Sanidad y Consumo adaptará al progreso científico el anexo II, teniendo en cuenta el principio de precaución y las evaluaciones realizadas por las organizaciones nacionales e internacionales competentes.

CAPITULO IV

Autorización e inspección de instalaciones radioeléctricas en relación con los límites de exposición

Artículo 8. *Determinados requisitos para la autorización, criterios de planificación e instalación de estaciones radioeléctricas.*

1. Los operadores que establezcan las redes o presten los servicios que se relacionan a continuación deberán presentar un estudio detallado, realizado por un técnico competente, que indique los niveles de exposición radioeléctrica en áreas cercanas a sus instalaciones radioeléctricas fijas en las que puedan permanecer habitualmente personas. Dichas redes o servicios son los siguientes:

a) Redes de difusión de los servicios de radiodifusión sonora y televisión.

b) Servicios de telefonía móvil automática analógica.

c) Servicio de telefonía móvil automática GSM.

d) Servicio de comunicaciones móviles personales DCS-1800.

e) Servicio de comunicaciones móviles de tercera generación.

f) Servicio de radiobúsqueda.

g) Servicio de comunicaciones móviles en grupo cerrado de usuarios.

h) Redes del servicio fijo por satélite, del servicio móvil por satélite y del servicio de radiodifusión por satélite.

i) Servicio de acceso vía radio LMDS.

Los mencionados niveles de exposición, valorados teniendo en cuenta el entorno radioeléctrico, deberán cumplir los límites establecidos en el anexo II de este Reglamento.

El citado estudio será presentado ante el Ministerio de Ciencia y Tecnología, incorporado en el proyecto o propuesta técnica necesarios para solicitar la autorización de las instalaciones radioeléctricas, según lo establecido en el capítulo I, título III, de la Orden de 9 de marzo de 2000, por la que se aprueba el Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.

2. Los operadores y titulares de licencias individuales a los que se refiere el apartado 1 presentarán, simultáneamente y de manera complementaria al estudio citado en dicho apartado, un proyecto de instalación de señalización y, en su caso, vallado que restrinja el acceso de personal no profesional a zonas en las que pudieran superarse las restricciones establecidas en el anexo II. Dicha señalización o vallado deberá estar instalado de manera previa a la puesta en servicio de la instalación radioeléctrica.

3. El Ministerio de Ciencia y Tecnología podrá ampliar la obligación prevista en los apartados anteriores a las solicitudes de autorización de otras instalaciones radioeléctricas.

4. El Ministerio de Sanidad y Consumo tendrá acceso a la información que le resulte necesaria sobre los niveles de exposición a los que se refiere el apartado primero de este artículo. Las autoridades sanitarias de las Comunidades Autónomas serán informadas por el Ministerio de Sanidad y Consumo cuando lo soliciten.

5. Sin perjuicio de lo dispuesto en el apartado primero de este artículo, la aprobación definitiva de las instalaciones estará condicionada a la no superación de los límites de exposición recogidos en el anexo II de este Reglamento.

6. No podrán establecerse nuevas instalaciones radioeléctricas o modificarse las existentes cuando su funcionamiento pudiera suponer que se superen los límites de exposición recogidos en el anexo II de este Reglamento.

7. En la planificación de las instalaciones radioeléctricas, los titulares de las mismas deberán tener en consideración, entre otros criterios, los siguientes:

a) La ubicación, características y condiciones de funcionamiento de las estaciones radioeléctricas deben minimizar los niveles de exposición del público en general a las emisiones radioeléctricas con origen tanto en éstas como, en su caso, en los terminales asociados a las mismas, manteniendo una adecuada calidad del servicio.

b) En el caso de instalación de estaciones radioeléctricas en cubiertas de edificios residenciales, los titulares de instalaciones radioeléctricas procurarán, siempre que sea posible, instalar el sistema emisor de manera que el diagrama de emisión no incida sobre el propio edificio, terraza o ático.

c) La compartición de emplazamientos podría estar condicionada por la consiguiente concentración de emisiones radioeléctricas.

d) De manera particular, la ubicación, características y condiciones de funcionamiento de las estaciones radioeléctricas debe minimizar, en la mayor medida posible, los niveles de emisión sobre espacios sensibles, tales como escuelas, centros de salud, hospitales o parques públicos.

Artículo 9. *Inspección y certificación de las instalaciones radioeléctricas.*

1. Será requisito previo a la utilización del dominio público radioeléctrico por parte de los operadores a los que se refiere el apartado 1 del artículo 8 la inspección o reconocimiento satisfactorio de las instalaciones por los servicios técnicos del Ministerio de Ciencia y Tecnología, en los términos establecidos en el artículo 65 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

2. Las instalaciones radioeléctricas deben ser realizadas por instaladores de telecomunicación inscritos, para el tipo correspondiente, en el Registro de Instaladores de Telecomunicación, según lo dispuesto en el Real Decreto 279/1999, de 22 de febrero, por el que se aprueba el Reglamento Regulador de las Infraestructuras Comunes de Telecomunicaciones para el Acceso a los Servicios de Telecomunicación en el Interior de los Edificios y de la Actividad de Instalación de Equipos y Sistemas de Telecomunicaciones.

3. Los servicios técnicos del Ministerio de Ciencia y Tecnología elaborarán planes de inspección para comprobar la adaptación de las instalaciones a lo dispuesto en este Reglamento.

Asimismo, los operadores a los que se refiere el apartado 1 del artículo 8 deberán remitir al Ministerio de Industria, Turismo y Comercio, en el primer trimestre de cada año natural, una certificación emitida por un técnico competente de que se han respetado los límites de exposición establecidos en el anexo II durante el año anterior. Este ministerio podrá ampliar esta obligación a titulares de otras instalaciones radioeléctricas.

Con carácter anual, el Ministerio de Ciencia y Tecnología, sobre la base de los resultados obtenidos en las citadas inspecciones y a las certificaciones presentadas por los operadores, elaborará y hará público un informe sobre la exposición a emisiones radioeléctricas.

4. El Ministerio de Sanidad y Consumo tendrá acceso a información sobre el resultado de las inspecciones y certificaciones a que se refieren los apartados anteriores de este artículo. Las autoridades sanitarias de las Comunidades Autónomas serán informadas por el Ministerio de Sanidad y Consumo cuando lo soliciten.

CAPITULO V

Otras disposiciones

Artículo 10. *Otras restricciones a los niveles de emisiones radioeléctricas.*

Sin perjuicio de las demás limitaciones establecidas en este Reglamento, toda estación radioeléctrica vendrá limitada en sus niveles de emisión por cualquiera de las siguientes condiciones:

a) La existencia de interferencias perjudiciales o incompatibilidades con otros servicios de telecomunicación previamente autorizados o con otros servicios públicos esenciales.

b) Las limitaciones impuestas por el Cuadro Nacional de Atribución de Frecuencias.

c) La existencia, fuera de la zona de servicio autorizada a la estación, de niveles de intensidad de campo electromagnético superiores a los máximos establecidos.

Artículo 11. *Equipos y aparatos.*

Todos los equipos y aparatos que utilicen el espectro radioeléctrico deberán haber evaluado su conformidad y cumplir el resto de requisitos que le son aplicables, en los términos recogidos en los artículos 56 y 57 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y en el Real Decreto 1890/2000, de 20 de noviembre, por el que se aprueba el Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones.

Adicionalmente, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá establecer procedimientos de evaluación voluntaria, conforme a lo dispuesto en el artículo 35 del Reglamento aprobado por el citado Real Decreto 1890/2000. En dichos procedimientos se podrán definir los parámetros técnicos aplicables a la evaluación, así como la información a suministrar en el manual de usuario o en el embalaje de los equipos. El establecimiento de estos procedimientos voluntarios de evaluación no implicará, en ningún caso, una restricción u obstáculo a la puesta en el mercado o a la puesta en servicio de los correspondientes equipos o aparatos.

Los procedimientos de evaluación voluntaria que se establezcan definirán las especificaciones técnicas aplicables, cuyo cumplimiento podrá ser verificado, según el caso, por declaración de conformidad del fabricante del equipo o por pruebas realizadas por organismos externos acreditados.

Las especificaciones técnicas se definirán teniendo en cuenta las normas técnicas elaboradas por los siguientes organismos, con el orden de prelación que se enumera a continuación:

a) Las adoptadas por organismos europeos de normalización reconocidos: El Instituto Europeo de Normas de Telecomunicación (ETSI), el Comité Europeo de Normalización (CEN) y el Comité Europeo de Normalización Electrotécnica (CENELEC).

b) Las internacionales adoptadas por la Unión Internacional de Telecomunicaciones (UIT), la Organización Internacional de Normalización (ISO) o la Comisión Electrotécnica Internacional (CEI).

c) Las emanadas de organismos españoles de normalización y, en particular, de la Asociación Española de Normalización y Certificación (AENOR).

d) Las especificaciones técnicas que cuenten con amplia aceptación en la industria y hayan sido elaboradas por los correspondientes organismos internacionales.

Artículo 12. *Instalación de estaciones radioeléctricas en un mismo emplazamiento.*

En el supuesto de instalación de varias estaciones radioeléctricas de diferentes operadores dentro de un mismo emplazamiento, los operadores se facilitarán mutuamente o a través del gestor del emplazamiento los datos técnicos necesarios para realizar el estudio de que el conjunto de instalaciones del emplazamiento no supera los niveles radioeléctricos máximos establecidos en este Reglamento.

Artículo 13. *Régimen sancionador.*

1. De conformidad con el artículo 79.16 y el artículo 80.15 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, constituirán infracciones muy graves y graves los incumplimientos por los titulares de autorizaciones generales y licencias individuales de las condiciones esenciales que se les impongan. A dichos efectos y de conformidad con los apartados 4 y 9 del artículo 5 de la Orden de 22 de septiembre de 1998, por la que se establecen el régimen aplicable a las licencias individuales para servicios y redes de telecomunicaciones y las condiciones que deben cumplirse por sus titulares, tendrá la consideración de infracción, por incumplimiento de condiciones esenciales, efectuar emisiones radioeléctricas que no respeten los límites de exposición establecidos en el artículo 6 o incumplir las obligaciones de señalización o vallado de las instalaciones de acuerdo con lo previsto en el apartado 2 del artículo 8 de este Reglamento.

2. Sin perjuicio de lo dispuesto en el apartado anterior, las infracciones a que se refiere el citado artículo 79.16 podrán ser sancionadas por constituir un incumplimiento de las condiciones y requisitos técnicos aplicables al uso del dominio público radioeléctrico, conforme establece el artículo 23 de la Orden de 9 de marzo de 2000, por la que se aprueba el Reglamento de desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.

DISPOSICIÓN TRANSITORIA

Unica. *Certificación y señalización de instalaciones autorizadas.*

1. En el plazo de nueve meses, contado a partir de la entrada en vigor de este Reglamento, los operadores y titulares de licencias individuales a los que se refiere el apartado 1 del artículo 8, que dispongan de instalaciones radioeléctricas autorizadas con anterioridad a la fecha de entrada en vigor de este Reglamento, remitirán, al Ministerio de Ciencia y Tecnología, una certificación de la conformidad de dichas instalaciones con los límites de exposición establecidos en el anexo II de este Reglamento, expedida por técnico competente.

En caso de que transcurrido el citado plazo no se presentase la certificación correspondiente a una instalación radioeléctrica, se entenderá que ésta no está autorizada para su funcionamiento. La nueva puesta en servicio de esta instalación radioeléctrica deberá atenerse a lo establecido en los artículos 8 y 9 de este Reglamento.

2. En el plazo de un año, contando a partir de la entrada en vigor de este Reglamento, los operadores y titulares de licencias individuales a los que se refiere el apartado 1 del artículo 8, que dispongan de instalaciones radioeléctricas autorizadas con anterioridad a la fecha de entrada en vigor de este Reglamento, deberán tener adecuadas todas sus instalaciones radioeléctricas a lo previsto en el apartado 2 del artículo 8. Una vez concluida esta adecuación, lo comunicarán al Ministerio de Ciencia y Tecnología.

3. El Ministerio de Ciencia y Tecnología informará al Ministerio de Sanidad y Consumo sobre el grado de conformidad de las instalaciones radioeléctricas.

ANEXO I

Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas

1. De acuerdo con lo establecido en la disposición adicional tercera de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, se establecen tres tipos de limitaciones y servidumbres para las estaciones radioeléctricas a las que hace referencia el apartado 2 del artículo 48 de la citada Ley, que afectan a:

a) A la altura máxima de los edificios.Para distancias inferiores a 1.000 metros, desde el punto de ubicación de la estación radioeléctrica a proteger, el ángulo que forme, sobre la horizontal, la dirección de observación del punto más elevado de un edificio, desde la parte superior de las antenas receptoras de menor altura de la estación, será como máximo de 3 grados.

b) A la distancia mínima a la que podrán ubicarse industrias e instalaciones eléctricas de alta tensión y líneas férreas electrificadas.La máxima limitación exigible de separación entre una industria o una línea de alta tensión o una línea férrea electrificada y cualquiera de las antenas receptoras de la estación a proteger será de 1.000 metros.

c) A la distancia mínima a la que podrán instalarse transmisores radioeléctricos, con o sin condiciones radioeléctricas exigibles (CRE).En el siguiente cuadro se establecen las limitaciones máximas exigibles en distancia entre las antenas transmisoras de estaciones radioeléctricas y las antenas receptoras de la estación a proteger.

Para determinados servicios de radiocomunicación se podrá optar entre mantener las distancias mínimas establecidas sin CRE o reducir estas distancias con las CRE necesarias, según la siguiente distribución.

Gama de frecuencias (f) (MHz)	Tipo de servicio perturbador	Potencia radiada aparente del transmisor en la dirección a la estación a proteger (kW)	Máxima limitación exigible en distancia de separación entre antena Tx y estación a proteger (km)	o	Máxima limitación en distancia y condiciones radioeléctricas exigibles (CRE) (1) (km)
F ≤ 30	Radiodifusión	0,01 < P ≤ 1 1 < P ≤ 10 P > 10	2 10 20		
	Otros servicios	0,01 < P ≤ 1 P > 1	2 10	ó	1 y CRE 5 y CRE
30 < f ≤ 3000	Radiodifusión Radiolocalización Investigación espacial (sentio Tierra-espacio)	0,01 < P ≤ 1 1 < P ≤ 10 P > 10	1 2 5		
	Otros servicios	0,01 < P ≤ 1 P > 1	1 2	ó	0,3 y CRE 1 y CRE
f > 3000	Radiolocalización Investigación espacial (sentido Tierra-espacio)	0,001 < P ≤ 1 1 < P ≤ 10 P > 10	1 2 5		
	Otros servicios	0,001 < P	1	ó	0,2 y CRE

(1) Nota: las condiciones radioeléctricas exigibles (CRE), serán aquellas condiciones técnicas y de apantallamiento o protección que deban incluirse en las estaciones radioeléctricas a fin de que sus emisiones no perturben el normal funcionamiento de la estación a proteger.

En caso de existir controversia sobre el grado de perturbación admisible, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, establecerá la suficiencia o insuficiencia de las CRE.

En los casos de estaciones de comprobación técnica de emisiones, para el establecimiento de las CRE, dentro de las distancias mínimas establecidas en el cuadro anterior, se tendrán en cuenta, además, los límites establecidos en la Recomendación UIT-R SM-575.

Frecuencia fundamental (f)	Norma de intensidad de campo (mV/m)	Media cuadriática para más de una intensidad de campo fundamental (mV/m)
9 kHz ≤ f < 174 MHz	10	30
174 MHz ≤ f < 960 MHz	50	150

Nota: el valor de la media cuadrática de la intensidad de campo se aplica a señales múltiples, pero únicamente cuando todas ellas están dentro de la banda de paso de RF del receptor de comprobación técnica.

2. Por lo que respecta a las limitaciones de intensidad de campo eléctrico en las estaciones de alta sensibilidad dedicadas a la investigación en los campos de radioastronomía y astrofísica, estas limitaciones serán las siguientes:

A) Las estaciones dedicadas a observaciones radioastronómicas, en cada una de las bandas de frecuencias que se encuentran atribuidas al servicio de radioastronomía en conformidad con el Cuadro Nacional de Atribución de Frecuencias, estarán protegidas contra la interferencia perjudicial por los niveles de intensidad de campo que se indican a continuación:

34,2 dB(μV/m) en la banda de 1400 a 1427 MHz.
35,2 dB(μV/m) en la banda de 1610,6 a 1613,8 MHz.
35,2 dB(μV/m) en la banda de 1660 a 1670 MHz.
31,2 dB(μV/m) en la banda de 2690 a 2700 MHz.
25,2 dB(μV/m) en la banda de 4990 a 5000 MHz.
14,2 dB(μV/m) en la banda de 10,6 a 10,7 GHz.

10,2 dB(μV/m) en la banda de 15,35 a 15,4 GHz.
2,2 dB(μV/m) en la banda de 22,21 a 22,5 GHz.
1,2 dB(μV/m) en la banda de 23,6 a 24 GHz.
4,8 dB(μV/m) en la banda de 31,3 a 31,8 GHz.
8,8 dB(μV/m) en la banda de 42,5 a 43,5 GHz.
20,8 dB(μV/m) en la banda de 86 a 92 GHz.

B) Para la protección de las instalaciones de observatorios de astrofísica, la limitación de la intensidad de campo eléctrico, en cualquier frecuencia, será de 88,8 dB(μV/m) en la ubicación del observatorio. Para la determinación de la intensidad de campo se tendrán en cuenta las estaciones de radiocomunicaciones cuyas potencias radiadas aparentes en dirección a los observatorios sean superiores a 25 vatios y estén situadas en un círculo de 20 kilómetros de radio alrededor de la ubicación del observatorio de astrofísica o, en el caso de las Comunidades Autónomas insulares, las que estén situadas en la isla donde esté ubicado el observatorio. Para los cálculos se tendrán en cuenta sus características técnicas y, en particular, las de la antena transmisora y las condiciones de apantallamiento del terreno y protección radioeléctrica. En el caso de que los cálculos teóricos den como resultado una intensidad de campo eléctrico superior al límite fijado, podrán realizarse medidas de intensidad de campo en la ubicación de los observatorios con señales de prueba.

3. Para un mejor aprovechamiento del espectro radioeléctrico, el Ministerio de Ciencia y Tecnología podrá imponer en las instalaciones la utilización de aquellos elementos técnicos que mejoren la compatibilidad radioeléctrica entre estaciones.

ANEXO II

Límites de exposición a las emisiones radioeléctricas

1. Definiciones

A) Magnitudes físicas: En el contexto de la exposición a las emisiones radioeléctricas, se emplean habitualmente las siguientes magnitudes físicas:

La corriente de contacto (Ic) entre una persona y un objeto se expresa en amperios (A). Un objeto conductor en un campo eléctrico puede ser cargado por el campo.

La densidad de corriente (J) se define como la corriente que fluye por una unidad de sección transversal perpendicular a la dirección de la corriente, en un conductor volumétrico, como puede ser el cuerpo humano o parte de éste, expresada en amperios por metro cuadrado (A/m^2).

La intensidad de campo eléctrico es una magnitud vectorial (E) que corresponde a la fuerza ejercida sobre una partícula cargada independientemente de su movimiento en el espacio. Se expresa en voltios por metro (V/m).

La intensidad de campo magnético es una magnitud vectorial (H) que, junto con la inducción magnética, determina un campo magnético en cualquier punto del espacio. Se expresa en amperios por metro (A/m).

La densidad de flujo magnético o inducción magnética es una magnitud vectorial (B) que da lugar a una fuerza que actúa sobre cargas en movimiento, y se expresa en teslas (T). En espacio libre y en materiales biológicos, la densidad de flujo o inducción magnética y la intensidad de campo magnético se pueden intercambiar utilizando la equivalencia 1 A/m = 4 π 10^{-7} T.

La densidad de potencia (S) es la magnitud utilizada para frecuencias muy altas, donde la profundidad de penetración en el cuerpo es baja. Es la potencia radiante que incide perpendicular a una superficie, dividida por el área de la superficie, y se expresa en vatios por metro cuadrado (W/m^2).

La absorción específica de energía (SA, «specific energy absorption») se define como la energía absorbida por unidad de masa de tejido biológico, expresada en julios por kilogramo (J/kg). En esta recomendación se utiliza para limitar los efectos no térmicos de la radiación de microondas pulsátil.

El índice de absorción específica de energía (SAR, «specific energy absorption rate»), se define como potencia absorbida por unidad de masa de tejido corporal, cuyo promedio se calcula en la totalidad del cuerpo o en partes de éste, y se expresa en vatios por kilogramo (W/kg). El SAR de cuerpo entero es una medida ampliamente aceptada para relacionar los efectos térmicos adversos con la exposición a las emisiones radioeléctricas. Junto al SAR medio de cuerpo entero, los valores SAR locales son necesarios para evaluar y limitar una deposición excesiva de energía en pequeñas partes del cuerpo como consecuencia de unas condiciones especiales de exposición. Ejemplos de tales condiciones son: La exposición a las emisiones radioeléctricas en la gama baja de Mhz de una persona en contacto con la tierra, o las personas expuestas en el espacio adyacente a una antena.

De entre estas magnitudes, las que pueden medirse directamente son la densidad de flujo magnético, la corriente de contacto, la intensidad del campo eléctrico y la del campo magnético y la densidad de potencia.

B) Restricciones básicas y niveles de referencia: Para la aplicación de las restricciones basadas en la evaluación de los posibles efectos de las emisiones radioeléctricas sobre la salud, se ha de diferenciar las restricciones básicas de los niveles de referencia.

Restricciones básicas. Las restricciones de la exposición a los campos eléctricos, magnéticos y electromagnéticos variables en el tiempo, basadas directamente en los efectos sobre la salud conocidos y en consideraciones biológicas, reciben el nombre de «restricciones básicas». Dependiendo de la frecuencia del campo, las magnitudes físicas empleadas para especificar estas restricciones son la inducción magnética (B), la densidad de corriente (J), el índice de absorción específica de energía (SAR) o la densidad de potencia (S). La inducción magnética y la densidad de potencia se pueden medir con facilidad en los individuos expuestos.

Niveles de referencia. Estos niveles se ofrecen a efectos prácticos de evaluación de la exposición, para determinar la probabilidad de que se sobrepasen las restricciones básicas. Algunos niveles de referencia se derivan de las restricciones básicas pertinentes utilizando mediciones o técnicas computerizadas, y algunos se refieren a la percepción y a los efectos adversos indirectos de la exposición a las emisiones radioeléctricas. Las magnitudes derivadas son la intensidad de campo eléctrico (E), la intensidad de campo magnético (H), la inducción magnética (B), la densidad de potencia (S) y la corriente en extremidades (I_l). Las magnitudes que se refieren a la percepción y otros efectos indirectos son la corriente (de contacto) (I_c) y, para los campos pulsátiles, la absorción específica de energía (SA). En cualquier situación particular de exposición, los valores medidos o calculados de cualquiera de estas cantidades pueden compararse con el nivel de referencia adecuado. El cumplimiento del nivel de referencia garantizará el respeto de la restricción básica pertinente. Que el valor medido sobrepase el nivel de referencia no quiere decir necesariamente que se vaya a sobrepasar la restricción básica. Sin embargo, en tales circunstancias es necesario comprobar si ésta se respeta.

Algunas magnitudes, como la inducción magnética (B) y la densidad de potencia (S), sirven a determinadas frecuencias como restricciones básicas y como niveles de referencia.

Los límites de exposición a emisiones radioeléctricas a los que se refiere el Reglamento son los resultantes de aplicar las restricciones básicas y los niveles de referencia en zonas en las que pueda permanecer habitualmente el público en general, sin perjuicio de lo establecido en otras disposiciones específicas en el ámbito laboral.

2. Restricciones básicas

Dependiendo de la frecuencia, para especificar las restricciones básicas sobre los campos electromagnéticos se emplean las siguientes cantidades físicas (cantidades dosimétricas o exposimétricas):

a) Entre 0 y 1 Hz se proporcionan restricciones básicas de la inducción magnética para campos magnéticos estáticos (0 Hz) y de la densidad de corriente para campos variables en el tiempo de 1 Hz, con el fin de prevenir los efectos sobre el sistema cardiovascular y el sistema nervioso central.

b) Entre 1 Hz y 10 MHz se proporcionan restricciones básicas de la densidad de corriente para prevenir los efectos sobre las funciones del sistema nervioso.

c) Entre 100 kHz y 10 GHz se proporcionan restricciones básicas del SAR para prevenir la fatiga calorífica de cuerpo entero y un calentamiento local excesivo de los tejidos. En la gama de 100 kHz a 10 MHz se ofrecen restricciones de la densidad de corriente y del SAR.

d) Entre 10 GHz y 300 GHz se proporcionan restricciones básicas de la densidad de potencia, con el fin de prevenir el calentamiento de los tejidos en la superficie corporal o cerca de ella.

Las restricciones básicas expuestas en el cuadro 1 se han establecido teniendo en cuenta las variaciones que puedan introducir las sensibilidades individuales y las condiciones medioambientales, así como el hecho de que la edad y el estado de salud de los ciudadanos varían.

CUADRO 1

Restricciones básicas para campos eléctricos, magnéticos y electromagnéticos (0 Hz-300 GHz)

Gama de frecuencia	Inducción magnética (mT)	Densidad de corriente (mA/m^2) rms	SAR medio de cuerpo entero (W/kg)	SAR Localizado (cabeza y tronco) (W/kg)	SAR Localizado (miembros) (W/kg)	Densidad de potencia S (W/m^2)
0 Hz	40					
>0-1 Hz		8				
1-4 Hz-		8/f				
4-1.000Hz		2				
1.000 Hz-100 kHz		f/500				
100 kHz-10 MHz		f/500	0,08	2	4	
10 MHz-10 GHz			0,08	2	4	
10-300 GHz						10

Notas:

1. f es la frecuencia en Hz.

2. El objetivo de la restricción básica de la densidad de corriente es proteger contra los graves efectos de la exposición sobre los tejidos del sistema nervioso central en la cabeza y en el tronco, e incluye un factor de seguridad. Las restricciones básicas para los campos frecuencias muy bajas se basan en los efectos negativos establecidos en el sistema nervioso central. Estos efectos agudos son esencialmente instantáneos y no existe justificación científica para modificar las restricciones básicas en relación con las exposiciones de corta duración. Sin embargo, puesto que las restricciones básicas se refieren a los efectos negativos en el sistema nervioso central, estas restricciones básicas pueden permitir densidades más altas en los tejidos del cuerpo distintos de los del sistema nervioso central en iguales condiciones de exposición.

3. Dada la falta de homogeneidad eléctrica del cuerpo, debe calcularse el promedio de las densidades de corriente en una sección transversal de 1 cm^2 perpendicular a la dirección de la corriente.

4. Para frecuencias de hasta 100 kHz, los valores pico de densidad de corriente pueden obtenerse multiplicando el valor cuadrático medio (rms) por $\sqrt{2}$ ($\approx$1,414). Para pulsos de duración t_p, la frecuencia equivalente que ha de aplicarse en las restricciones básicas debe calcularse como $f = 1/(2t_p)$.

5. Para frecuencias de hasta 100 kHz y para campos magnéticos pulsátiles, la densidad de corriente máxima asociada con los pulsos puede calcularse a partir de los tiempos de subida/caída y del índice máximo de cambio de la inducción magnética. La densidad de corriente inducida puede entonces compararse con la restricción básica correspondiente.

6. Todos los valores SAR deben ser promediados a lo largo de un período cualquiera de seis minutos.

7. La masa promediada de SAR localizado la constituye una porción cualquiera de 10 g de tejido contiguo; el SAR máximo obtenido de esta forma debe ser el valor que se utilice para evaluar la exposición. Estos 10 g de tejido se consideran como una masa de tejidos

contiguos con propiedades eléctricas casi homogéneas. Especificando que se trata de una masa de tejidos contiguos, se reconoce que este concepto puede utilizarse en la dosimetría automatizada, aunque puede presentar dificultades a la hora de efectuar mediciones físicas directas. Puede utilizarse una geometría simple, como una masa de tejidos cúbica, siempre que las cantidades dosimétricas calculadas tengan valores de prudencia en relación con las directrices de exposición.

8. Para los pulsos de duración tp, la frecuencia equivalente que ha de aplicarse en las restricciones básicas debe calcularse como $f = 1/(2t_p)$. Además, en lo que se refiere a las exposiciones pulsátiles, en la gama de frecuencias de 0,3 a 10 GHz y en relación con la exposición localizada de la cabeza, la SA no debe sobrepasar los 2 mJ/kg^{-1} como promedio calculado en 10 g de tejido.

3. Niveles de referencia.

Los niveles de referencia de la exposición sirven para ser comparados con los valores de las magnitudes medidas. El respeto de todos los niveles de referencia asegurará el respeto de las restricciones básicas.

Si las cantidades de los valores medidos son mayores que los niveles de referencia, no significa necesariamente que se hayan sobrepasado las restricciones básicas. En este caso, debe efectuarse una evaluación para comprobar si los niveles de exposición son inferiores a las restricciones básicas.

Los niveles de referencia para limitar la exposición se obtienen a partir de las restricciones básicas, presuponiendo un acoplamiento máximo del campo con el individuo expuesto, con lo que se obtiene un máximo de protección. En los cuadros 2 y 3 figura un resumen de los niveles de referencia. Por lo general, éstos están pensados como valores promedio, calculados espacialmente sobre toda la extensión del cuerpo del individuo expuesto, pero teniendo muy en cuenta que no deben sobrepasarse las restricciones básicas de exposición localizadas.

En determinadas situaciones en las que la exposición está muy localizada, como ocurre con los teléfonos móviles y con la cabeza del individuo, no es apropiado emplear los niveles de referencia. En estos casos, debe evaluarse directamente si se respeta la restricción básica localizada.

3.1 Niveles de campo.

CUADRO 2

Niveles de referencia para campos eléctricos, magnéticos y electromagnéticos (0 Hz-300 GHz, valores rms imperturbados)

Gama de frecuencia	Intensidad de campo E (V/m)	Intensidad de campo H (A/m)	Campo B (μT)	Densidad de potencia equivalente de onda plana (W/m^2)
0-1 Hz		$3,2 \times 10^4$	4×10^4	
1-8 Hz	10.000	$3,2 \times 10^4/f^2$	$4 \times 10^4/f^2$	
8-25 Hz	10.000	4.000/f	5.000/f	
0,025-0,8 kHz	250/f	4/f	5/f	
0,8-3 kHz	250/f	5	6,25	
3-150 kHz	87	5	6,25	
0,15-1 MHz	87	0,73/f	0,92/f	
1-10 MHz	$87/f^{1/2}$	0,73/f	0,92/f	
10-400 MHz	28	0,073	0,092	2
400-2.000 MHz	$1,375\ f^{1/2}$	$0,0037\ f^{1/2}$	$0,0046\ f^{1/2}$	f/200
2-300 GHz	61	0,16	0,20	10

Notas:

1. f según se indica en la columna de gama de frecuencia.

2. Para frecuencias de 100 kHz a 10 GHz, el promedio de S_{eq}, E^2, H^2 y B^2, ha de calcularse a lo largo de un período cualquiera de seis minutos.

3. Para frecuencias superiores a 10 GHz, el promedio de S_{eq}, E^2, H^2 y B^2, ha de calcularse a lo largo de un período cualquiera de $68/f^{1,05}$ minutos (f en GHz).

4. No se ofrece ningún valor de campo E para frecuencias <1 Hz. La mayor parte de las personas no percibirá las cargas eléctricas superficiales con resistencias de campo inferiores a 25 kV/m. En cualquier caso, deben evitarse las descargas de chispas, que causan estrés o molestias.

Nota: no se indican niveles de referencia más altos para la exposición a los campos de frecuencia extremadamente baja (FEB) cuando las exposiciones son de corta duración (véase nota 2 del cuadro 1). En muchos casos, cuando los valores medidos rebasan el nivel de referencia, no se deduce necesariamente que se haya rebasado la restricción básica. Siempre que puedan evitarse los impactos negativos para la salud de los efectos indirectos de la exposición (como los microshocks), se reconoce que pueden rebasarse los niveles de referencia, siempre que no se rebase la restricción básica relativa a la densidad de corriente.

En cuanto a valores de pico, se aplicarán los siguientes niveles de referencia para la intensidad de campo eléctrico (E) (V/m), la intensidad de campo magnético (H) (A/m) y a la inducción de campo magnético (B) (μT):

a) Para frecuencias de hasta 100 kHz, los valores de pico esta de referencia se obtienen multiplicando los valores rms correspondientes por $\sqrt{2}$ (≈1,414). Para pulsos de duración t_p, la frecuencia equivalente que ha de aplicarse debe calcularse como $f=1/(2t_p)$.

b) Para frecuencias de entre 100 kHz y 10 MHz, los valores de pico de referencia se obtienen multiplicando los valores rms correspondientes por 10^a, donde $a = [0,665 \log (f/10^5) + 0,176]$, donde f se expresa en Hz.

c) Para frecuencias de entre 10 MHz y 300 GHz, los valores de referencia de pico se obtienen multiplicando los valores rms correspondientes por 32.

Nota: en lo que se refiere a frecuencias que sobrepasan los 10 MHz, el promedio Seq calculado en la anchura del pulso no debe ser mayor de 1.000 veces los niveles de referencia, o bien las intensidades de campo no deben ser mayores de 32 veces los niveles de referencia de intensidad de campo. Para frecuencias de entre unos 0,3 GHz y varios GHz, y en relación con la exposición localizada de la cabeza, debe limitarse la absorción específica derivada de los pulsos, para limitar o evitar los efectos auditivos causados por la extensión termoelástica. En esta gama de frecuencia, el umbral SA de 4-16 mJ/kg^{-1} que es necesario para producir este efecto corresponde, para pulsos 30μS, a valores máximos SAR de 130 a 520 W/kg^{-1} en el cerebro. Entre 100 kHz y 10 MHz, los valores de pico de las intensidades de campo se obtienen mediante interpolación desde el pico multiplicado por 1,5 a 100 kHz hasta el pico multiplicado por 32 a 10 MHz.

3.2 Corrientes de contacto y corriente en extremidades: Para frecuencias de hasta 110 MHz se establecen niveles de referencia adicionales para evitar los peligros debidos a las corrientes de contacto. En el cuadro 3 figuran los niveles de referencia de corriente de contacto. Éstos se han establecido para tomar en consideración el hecho de que las corrientes de contacto umbral que provocan reacciones biológicas en mujeres adultas y niños, equivalen aproximadamente a dos tercios y la mitad, respectivamente, de las que corresponden a hombres adultos.

CUADRO 3

Niveles de referencia para corrientes de contacto procedentes de objetos conductores (f en kHz)

Gama de frecuencia	Corriente máxima de contacto (mA)
0 Hz-2,5 kHz	0,5
2,5 KHz-100 kHz	0,2 f
100 KHz-110 MHz	20

Para la gama de frecuencias de 10 MHz a 110 MHz, se establece un nivel de referencia 45 mA en términos de corriente a través de cualquier extremidad. Con ello, se pretende limitar el SAR localizado a lo largo de un período cualquiera de seis minutos.

4. Exposición a fuentes con múltiples frecuencias. En situaciones en las que se da una exposición simultánea a campos de diferentes frecuencias, debe tenerse en cuenta la posibilidad de que se sumen los efectos de estas exposiciones. Para cada efecto deben hacerse cálculos basados en esa actividad; así pues, deben efectuarse evaluaciones separadas de los efectos de la estimulación térmica y eléctrica sobre el cuerpo.

4.1 Restricciones básicas:

En el caso de la exposición simultánea a campos de diferentes frecuencias, deberán cumplirse los siguientes criterios como restricciones básicas.

En cuanto a la estimación eléctrica, pertinente en lo que se refiere a frecuencias de 1 Hz a 10 MHz, las densidades de corriente inducida deben cumplir lo siguiente:

$$\left| \sum_{i=1\,Hz}^{10\,MHz} \frac{J_i}{J_{L,i}} \leq 1 \right|$$

donde:

J_i es la densidad de corriente a la frecuencia i;

$J_{L,i}$ es la restricción básica de densidad de corriente a la frecuencia i, según figura en el cuadro1;

En lo que respecta a los efectos térmicos, pertinentes a partir de los 100 kHz, los índices de absorción específica de energía y las densidades de potencia deben cumplir lo siguiente:

$$\left| \sum_{i=100\,kHz}^{10GHz} \frac{SAR_i}{SAR_L} + \sum_{i>10GHz}^{300GHz} \frac{S_i}{S_L} \leq 1 \right|$$

donde:

SAR_i es el SAR causado por la exposición a la frecuencia i;

SAR_L es la restricción básica de SAR que figura en el cuadro 1;

S_i es la densidad de potencia a la frecuencia i;

S_L es la restricción básica de densidad de potencia que figura en el cuadro 1.

4.2 Niveles de referencia:

1.º Para la aplicación práctica de las restricciones básicas deben considerarse los siguientes criterios relativos a los niveles de referencia de las intensidades de campo.

En relación con las densidades de corriente inducida y los efectos de estimulación eléctrica, pertinentes hasta los 10 MHz, a los niveles de campo deben aplicarse las dos exigencias siguientes:

$$\sum_{i=1\,Hz}^{1\,MHz} \frac{E_i}{E_{L,i}} + \sum_{i>1\,MHz}^{10\,MHz} \frac{E_i}{a} \leq 1$$

$$\sum_{j=1\,Hz}^{150\,kHz} \frac{H_j}{H_{L,j}} + \sum_{j>150\,kHz}^{10\,MHz} \frac{H_j}{b} \leq 1$$

donde:

E_i es la intensidad de campo eléctrico a la frecuencia i;

$E_{L,i}$ es el nivel de referencia de campo eléctrico del cuadro 2;

H_j es la densidad de campo magnético a la frecuencia j;

$H_{L,j}$ es el nivel de referencia de campo magnético derivado del cuadro 2;

a es 87 V/m y b es 5 A/m (6,25 μT).

El uso de los valores constantes (a y b) por encima de 1 MHz en lo que respecta al campo eléctrico, y por encima de 150 kHz en lo que se refiere al campo magnético, se debe al hecho de que la suma está basada en densidades de corriente inducida y no debe mezclarse con las circunstancias de efectos térmicos. Esto último constituye la base para $E_{L,i}$ y $H_{L,j}$ por encima de 1 MHz y 150 kHz, respectivamente, que figuran en el cuadro 2.

En relación con las circunstancias de efecto térmico, pertinentes a partir de 100 kHz, a los niveles de campo deben aplicarse las dos exigencias siguientes:

$$\sum_{i=100kHz}^{1MHz}\left(\frac{E_i}{c}\right)^2+\sum_{i>1MHz}^{300GHz}\left(\frac{E_i}{E_{L,i}}\right)^2\leq 1$$

$$\sum_{j=100kHz}^{150kHz}\left(\frac{H_j}{d}\right)^2+\sum_{j>150kHz}^{300GHz}\left(\frac{H_j}{H_{L,j}}\right)^2\leq 1$$

donde:

E_j es la intensidad de campo eléctrico a la frecuencia i;
$E_{L,i}$ es el nivel de referencia de campo eléctrico del cuadro 2;
H_j es la densidad de campo magnético a la frecuencia j;
$H_{L,j}$ es el nivel de referencia de campo magnético derivado del cuadro 2;
c es 87/f1/2 V/m y d 0,73/f A/m, donde f es la frecuencia expresada en MHz.

2.º Para la corriente de extremidades y la corriente de contacto, respectivamente, deben aplicarse las siguientes exigencias:

$$\sum_{k=10MHz}^{110MHz}\left(\frac{I_k}{I_{L,k}}\right)^2\leq 1;\ \sum_{n\rangle 1Hz}^{110MHz}\left(\frac{I_n}{I_{C,n}}\right)^2\leq 1$$

donde:

I_k es el componente de corriente de extremidades a la frecuencia k;
$I_{L,k}$ es el nivel de referencia de la corriente de extremidades, 45 mA;
I_n es el componente de corriente de contacto a la frecuencia n;
$I_{C,n}$ es el nivel de referencia de la corriente de contacto a la frecuencia n (véase el cuadro 3);

Las anteriores fórmulas de adición presuponen las peores condiciones de fase entre los campos. En consecuencia, las situaciones típicas de exposición pueden dar lugar, en la práctica, a unos niveles de exposición menos restrictivos de lo que indican las fórmulas correspondientes a los niveles de referencia.

5. Métodos de medida y referencias.

En lo relativo a los métodos de medidas, tipos de instrumentación y otros requisitos se estará a lo recogido en las normas técnicas aplicables, con el orden de prelación que figura en el artículo 11.

§ 36

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Jefatura del Estado
«BOE» núm. 251, de 19 de octubre de 2007
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2007-18243

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por

agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.
2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.
3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.
4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada

mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los

Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 37

Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados

Ministerio de la Presidencia
«BOE» núm. 40, de 15 de febrero de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-1591

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Esta Ley se aplica a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. Se excluye del ámbito de aplicación de la citada Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

La Ley 25/2007, de 18 de octubre, enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

La disposición adicional única de la Ley 25/2007, de 18 de octubre, a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, establece, como obligación

de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Asimismo, la citada Ley 25/2007, de 18 de octubre, establece en su disposición final cuarta, relativa al formato de entrega de los datos, que la cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda. La citada habilitación normativa a favor del Ministerio de Defensa debe entenderse residenciada actualmente en el Ministerio de la Presidencia, puesto que el Centro Nacional de Inteligencia, del cual se deriva su afección, ha pasado a depender de este último Departamento, en virtud de lo establecido en la disposición adicional segunda del Real Decreto 1823/2011, de 21 de diciembre, por el que se reestructuran los Departamentos Ministeriales. Y por idénticos motivos de reestructuración orgánica, la referencia al Ministerio de Economía y Hacienda deba entenderse encuadrada en el ámbito competencial del Ministerio de Hacienda y Administraciones Públicas.

Esta Orden tiene por objeto el establecimiento de las especificaciones técnicas del formato de entrega a los agentes facultados de los datos conservados por los operadores que son generados y tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación.

Se adopta el modelo promovido por el ETSI (Instituto Europeo de Normalización de las Telecomunicaciones) para el establecimiento de dichas especificaciones. Este modelo consiste en un conjunto de normas elaboradas en el seno de este organismo de normalización en el que participan expertos de todos los sectores involucrados en la retención de datos, lo que garantiza un elevado nivel de consenso y de calidad de las normas desarrolladas, así como el mantenimiento y la adaptación a las diferentes tecnologías de telecomunicaciones que vayan surgiendo en el mercado.

La adopción del modelo ETSI implica la incorporación a la legislación española de una especificación técnica del ETSI que especifica el flujo de información así como los procedimientos, formatos y protocolos específicos de las interfaces de entrega (HI) entre los sujetos obligados y los agentes facultados: ETSI TS 102 657.

Finalmente, la presente Orden ha sido sometida al previo informe de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en los artículos 37.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y 5.b) del Estatuto de la Agencia, aprobado por el Real Decreto 428/1993, de 26 de marzo.

En su virtud, a propuesta de este Ministerio y de los Ministros del Interior, de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

Constituye el objeto de esta orden el establecimiento de las especificaciones técnicas del formato de entrega a los agentes facultados de los datos objeto de conservación a que hace referencia el artículo 3 y la disposición adicional única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de acuerdo con lo establecido en la disposición final cuarta de dicha Ley.

Lo dispuesto en esta orden se entiende sin perjuicio de los desarrollos reglamentarios previstos en la disposición final tercera de la mencionada Ley.

Estarán obligados a seguir los procedimientos y adoptar las medidas a las que se refiere la presente orden ministerial los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones en España, con independencia de la naturaleza, ámbito territorial y momento que tuvo efecto su habilitación, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Formato de entrega de los datos a los agentes facultados.*

1. Número de solicitudes individuales de cesión de datos entre todos los agentes facultados superior a 2.000.–En el marco de la Ley 25/2007, de 18 de octubre, la cesión a los agentes facultados de los datos cuya conservación sea obligatoria por parte de los operadores, se efectuará, cuando el número de solicitudes individuales de cesión de datos

entre todos los agentes facultados sea superior a 2.000 solicitudes durante el año natural anterior a la entrada en vigor de la presente orden ministerial, según el formato establecido en la especificación técnica del Instituto Europeo de Normalización de las Telecomunicaciones (ETSI) TS 102 657, Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data, con las modificaciones y precisiones que se establecen en el anexo I de esta orden ministerial.

2. Número de solicitudes individuales de cesión de datos entre todos los agentes facultados igual o inferior a 2.000.–Cuando un sujeto obligado haya recibido un número de solicitudes individuales de cesión de datos entre todos los agentes facultados igual o inferior a 2.000 solicitudes durante el año natural anterior a la entrada en vigor de la presente orden ministerial, o en años naturales posteriores se viera disminuido el número de las mismas por debajo de las ya citadas 2.000 solicitudes, en lugar de utilizar el formato de entrega basado en la norma ETSI TS 102 657 podrá optar por utilizar otra solución tecnológica acordada previamente con los agentes facultados de entre los diferentes formatos especificados para este caso en el anexo III, en formato electrónico y cuyo nombre se adecuará a lo definido en el punto 7.1 del anexo I de esta Orden ministerial.

Para poder optar a esta solución, el sujeto obligado deberá comunicar a cada agente facultado que no se han superado en el año natural anterior las 2.000 solicitudes individuales y su petición de acogerse a la solución tecnológica alternativa previamente acordada. En todo caso la solución tecnológica acordada deberá garantizar el cumplimiento de las medidas de seguridad exigibles conforme a lo establecido en la normativa de protección de datos de carácter personal.

Si en el primer caso no se alcanzara el acuerdo preceptivo entre el sujeto obligado y los agentes facultados o si establecida la excepción contemplada en el segundo caso se superara posteriormente el número de 2.000 solicitudes, se aplicará lo establecido en el apartado 1 de este artículo.

3. Plazo de adopción del formato de entrega.–Cuando un sujeto obligado haya recibido un número superior a 2.000 solicitudes individuales de cesión de datos durante el año natural anterior a la entrada en vigor de la presente orden ministerial o acordada la excepción del apartado 2 de este artículo se superara posteriormente el número de 2.000 solicitudes dentro de un año natural, dispondrá del plazo fijado por la Ley 25/2007, de 18 de octubre, en su disposición final cuarta, para implantar el procedimiento de cesión basado en la norma ETSI TS 102 657 adoptado en esta orden. Dicho plazo se contabilizará desde la entrada en vigor de la presente orden ministerial en el primer caso y desde el momento en el que se supere el número de 2.000 solicitudes dentro de un año natural en el segundo.

Artículo 3. *Información de localización.*

Los sujetos obligados que presten servicios móviles deberán proveer la información de localización del terminal móvil solicitada, de acuerdo con lo establecido en el anexo I de esta orden.

Artículo 4. *Canales de comunicaciones entre sujetos obligados y agentes facultados.*

Existirán dos tipos de canales de comunicaciones entre cada sujeto obligado y cada agente facultado para la entrega de los datos solicitados: un canal para intercambio de información administrativa sobre peticiones/respuestas (Interfaz HI-A), y otro canal para transmitir los datos retenidos por el sujeto obligado (Interfaz HI-B). Estos dos canales «lógicos» podrán ser realizados sobre el mismo canal «físico» de enlace, y en cualquier caso se encontrarán, obligatoriamente, dentro del territorio nacional.

El anexo II de esta orden recoge las características y requisitos que deben cumplir ambos canales de comunicaciones así como los pormenores del abono del coste de las comunicaciones por parte de los agentes facultados.

Artículo 5. *Comunicación de información relacionada con la de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones entre sujetos obligados.*

1. La información relacionada con el mandamiento de la conservación de datos, relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que se intercambie entre sujetos obligados, se limitará a la estrictamente necesaria para satisfacer las necesidades derivadas de la obligación de colaborar entre operadores para la realización de la misma. Los sujetos obligados garantizarán en todo momento la confidencialidad de la información transmitida o almacenada, no pudiendo ser utilizada para ningún otro fin. En todo caso conforme a las exigencias de la Ley 25/2007, de 18 de octubre, este intercambio de información en modo alguno podrá referirse a los datos de carácter personal respecto de los que existe la obligación de conservación y, en su caso, comunicación a los agentes facultados.

2. Las órdenes de cesión de los datos conservados y cualquier otra información importante para la seguridad del sistema de conservación, debe transmitirse mediante un canal seguro, según se define en el anexo II de esta orden.

Disposición transitoria única. *Plazo para el cumplimiento.*

Los sujetos obligados que estén prestando servicio a la entrada en vigor de la presente orden ministerial deberán cumplir las obligaciones establecidas en la misma en el plazo fijado por la Ley 25/2007, de 18 de octubre, en su disposición final cuarta, conforme a lo dispuesto en el artículo 2 de esta orden ministerial.

Aquellos sujetos obligados que inicien su actividad con posterioridad a la entrada en vigor de esta orden ministerial, deberán cumplir las obligaciones establecidas en esta orden ministerial desde el inicio de su actividad, pudiéndose acoger a lo dispuesto en el párrafo segundo del artículo 2 cuando se verifiquen dichas condiciones a la finalización del primer año natural completo desde el inicio de su actividad.

Disposición final primera. *Habilitación normativa.*

Se faculta a los titulares de la Secretaría de Estado de Seguridad, de la Secretaría de Estado Director del Centro Nacional de Inteligencia (CNI) y de la Secretaría de Estado de Hacienda para actualizar conjuntamente el contenido de los anexos de la presente Orden.

Disposición final segunda. *Impacto presupuestario en la Administración Pública.*

Las previsiones contenidas en esta orden no supondrán incremento de gastos de personal por ningún concepto y se llevarán a cabo con los medios personales disponibles en los departamentos ministeriales y organismos interesados.

Disposición final tercera. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXOS

[Anexos I, II y III omitidos. Consúltese el PDF oficial.]

§ 38

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 281, de 24 de noviembre de 1995
Última modificación: 28 de abril de 2015
Referencia: BOE-A-1995-25444

[. . .]

LIBRO I

Disposiciones generales sobre los delitos, las personas responsables, las penas, medidas de seguridad y demás consecuencias de la infracción penal.

[. . .]

TÍTULO II

De las personas criminalmente responsables de los delitos

Artículo 27.

Son responsables criminalmente de los delitos los autores y los cómplices.

Artículo 28.

Son autores quienes realizan el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento.

También serán considerados autores:

a) Los que inducen directamente a otro u otros a ejecutarlo.

b) Los que cooperan a su ejecución con un acto sin el cual no se habría efectuado.

Artículo 29.

Son cómplices los que, no hallándose comprendidos en el artículo anterior, cooperan a la ejecución del hecho con actos anteriores o simultáneos.

Artículo 30.

1. En los delitos que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente.

2. Los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden:

1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo.

2.º Los directores de la publicación o programa en que se difunda.

3.º Los directores de la empresa editora, emisora o difusora.

4.º Los directores de la empresa grabadora, reproductora o impresora.

3. Cuando por cualquier motivo distinto de la extinción de la responsabilidad penal, incluso la declaración de rebeldía o la residencia fuera de España, no pueda perseguirse a ninguna de las personas comprendidas en alguno de los números del apartado anterior, se dirigirá el procedimiento contra las mencionadas en el número inmediatamente posterior.

Artículo 31.

El que actúe como administrador de hecho o de derecho de una persona jurídica, o en nombre o representación legal o voluntaria de otro, responderá personalmente, aunque no concurran en él las condiciones, cualidades o relaciones que la correspondiente figura de delito requiera para poder ser sujeto activo del mismo, si tales circunstancias se dan en la entidad o persona en cuyo nombre o representación obre.

Artículo 31 bis.

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:

1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;

2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;

3.ª los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y

4.ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª

En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.

4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.

5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

Artículo 31 ter.

1. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el artículo anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.

2. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el artículo siguiente.

Artículo 31 quater.

1. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:

a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.

b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos.

c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito.

d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.

Artículo 31 quinquies.

1. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas.

2. En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33. Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

[. . .]

TÍTULO V

De la responsabilidad civil derivada de los delitos y de las costas procesales

CAPÍTULO I

De la responsabilidad civil y su extensión

Artículo 109.

1. La ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados.

2. El perjudicado podrá optar, en todo caso, por exigir la responsabilidad civil ante la Jurisdicción Civil.

Artículo 110.

La responsabilidad establecida en el artículo anterior comprende:

1.º La restitución.
2.º La reparación del daño.
3.º La indemnización de perjuicios materiales y morales.

Artículo 111.

1. Deberá restituirse, siempre que sea posible, el mismo bien, con abono de los deterioros y menoscabos que el juez o tribunal determinen. La restitución tendrá lugar aunque el bien se halle en poder de tercero y éste lo haya adquirido legalmente y de buena fe, dejando a salvo su derecho de repetición contra quien corresponda y, en su caso, el de ser indemnizado por el responsable civil del delito.

2. Esta disposición no es aplicable cuando el tercero haya adquirido el bien en la forma y con los requisitos establecidos por las Leyes para hacerlo irreivindicable.

Artículo 112.

La reparación del daño podrá consistir en obligaciones de dar, de hacer o de no hacer que el Juez o Tribunal establecerá atendiendo a la naturaleza de aquél y a las condiciones personales y patrimoniales del culpable, determinando si han de ser cumplidas por él mismo o pueden ser ejecutadas a su costa.

Artículo 113.

La indemnización de perjuicios materiales y morales comprenderá no sólo los que se hubieren causado al agraviado, sino también los que se hubieren irrogado a sus familiares o a terceros.

Artículo 114.

Si la víctima hubiere contribuido con su conducta a la producción del daño o perjuicio sufrido, los Jueces o Tribunales podrán moderar el importe de su reparación o indemnización.

Artículo 115.

Los Jueces y Tribunales, al declarar la existencia de responsabilidad civil, establecerán razonadamente, en sus resoluciones las bases en que fundamenten la cuantía de los daños e indemnizaciones, pudiendo fijarla en la propia resolución o en el momento de su ejecución.

CAPÍTULO II

De las personas civilmente responsables

Artículo 116.

1. Toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que deba responder cada uno.

2. Los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables.

La responsabilidad subsidiaria se hará efectiva: primero, en los bienes de los autores, y después, en los de los cómplices.

Tanto en los casos en que se haga efectiva la responsabilidad solidaria como la subsidiaria, quedará a salvo la repetición del que hubiere pagado contra los demás por las cuotas correspondientes a cada uno.

3. La responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil en los términos establecidos en el artículo 110 de este Código de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos.

Artículo 117.

Los aseguradores que hubieren asumido el riesgo de las responsabilidades pecuniarias derivadas del uso o explotación de cualquier bien, empresa, industria o actividad, cuando, como consecuencia de un hecho previsto en este Código, se produzca el evento que determine el riesgo asegurado, serán responsables civiles directos hasta el límite de la indemnización legalmente establecida o convencionalmente pactada, sin perjuicio del derecho de repetición contra quien corresponda.

Artículo 118.

1. La exención de la responsabilidad criminal declarada en los números 1.º, 2.º, 3.º, 5.º y 6.º del artículo 20, no comprende la de la responsabilidad civil, que se hará efectiva conforme a las reglas siguientes:

1.ª En los casos de los números 1.º y 3.º, son también responsables por los hechos que ejecuten los declarados exentos de responsabilidad penal quienes los tengan bajo su potestad o guarda legal o de hecho, siempre que haya mediado culpa o negligencia por su parte y sin perjuicio de la responsabilidad civil directa que pudiera corresponder a los imputables.

Los Jueces o Tribunales graduarán de forma equitativa la medida en que deba responder con sus bienes cada uno de dichos sujetos.

2.ª Son igualmente responsables el ebrio y el intoxicado en el supuesto del número 2.º

3.ª En el caso del número 5.º serán responsables civiles directos las personas en cuyo favor se haya precavido el mal, en proporción al perjuicio que se les haya evitado, si fuera estimable o, en otro caso, en la que el Juez o Tribunal establezca según su prudente arbitrio.

Cuando las cuotas de que deba responder el interesado no sean equitativamente asignables por el Juez o Tribunal, ni siquiera por aproximación, o cuando la responsabilidad se extienda a las Administraciones Públicas o a la mayor parte de una población y, en todo caso, siempre que el daño se haya causado con asentimiento de la autoridad o de sus agentes, se acordará, en su caso, la indemnización en la forma que establezcan las leyes y reglamentos especiales.

4.ª En el caso del número 6.º, responderán principalmente los que hayan causado el miedo, y en defecto de ellos, los que hayan ejecutado el hecho.

2. En el caso del artículo 14, serán responsables civiles los autores del hecho.

Artículo 119.

En todos los supuestos del artículo anterior, el Juez o Tribunal que dicte sentencia absolutoria por estimar la concurrencia de alguna de las causas de exención citadas, procederá a fijar las responsabilidades civiles salvo que se haya hecho expresa reserva de las acciones para reclamarlas en la vía que corresponda.

Artículo 120.

Son también responsables civilmente, en defecto de los que lo sean criminalmente:

1.º Los padres o tutores, por los daños y perjuicios causados por los delitos cometidos por los mayores de dieciocho años sujetos a su patria potestad o tutela y que vivan en su compañía, siempre que haya por su parte culpa o negligencia.

2.º Las personas naturales o jurídicas titulares de editoriales, periódicos, revistas, estaciones de radio o televisión o de cualquier otro medio de difusión escrita, hablada o visual, por los delitos cometidos utilizando los medios de los que sean titulares, dejando a salvo lo dispuesto en el artículo 212.

3.º Las personas naturales o jurídicas, en los casos de delitos cometidos en los establecimientos de los que sean titulares, cuando por parte de los que los dirijan o administren, o de sus dependientes o empleados, se hayan infringido los reglamentos de policía o las disposiciones de la autoridad que estén relacionados con el hecho punible cometido, de modo que éste no se hubiera producido sin dicha infracción.

4.º Las personas naturales o jurídicas dedicadas a cualquier género de industria o comercio, por los delitos que hayan cometido sus empleados o dependientes, representantes o gestores en el desempeño de sus obligaciones o servicios.

5.º Las personas naturales o jurídicas titulares de vehículos susceptibles de crear riesgos para terceros, por los delitos cometidos en la utilización de aquellos por sus dependientes o representantes o personas autorizadas.

Artículo 121.

El Estado, la Comunidad Autónoma, la provincia, la isla, el municipio y demás entes públicos, según los casos, responden subsidiariamente de los daños causados por los penalmente responsables de los delitos dolosos o culposos, cuando éstos sean autoridad, agentes y contratados de la misma o funcionarios públicos en el ejercicio de sus cargos o funciones siempre que la lesión sea consecuencia directa del funcionamiento de los servicios públicos que les estuvieren confiados, sin perjuicio de la responsabilidad patrimonial derivada del funcionamiento normal o anormal de dichos servicios exigible conforme a las normas de procedimiento administrativo, y sin que, en ningún caso, pueda darse una duplicidad indemnizatoria.

Si se exigiera en el proceso penal la responsabilidad civil de la autoridad, agentes y contratados de la misma o funcionarios públicos, la pretensión deberá dirigirse simultneamente contra la Administración o ente público presuntamente responsable civil subsidiario.

Artículo 122.

El que por título lucrativo hubiere participado de los efectos de un delito, está obligado a la restitución de la cosa o al resarcimiento del daño hasta la cuantía de su participación.

[. . .]

CAPÍTULO II

De las amenazas

Artículo 169.

El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.

Artículo 170.

1. Si las amenazas de un mal que constituyere delito fuesen dirigidas a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, o colectivo social o profesional, o a cualquier otro grupo de personas, y tuvieran la gravedad necesaria para conseguirlo, se impondrán respectivamente las penas superiores en grado a las previstas en el artículo anterior.

2. Serán castigados con la pena de prisión de seis meses a dos años, los que, con la misma finalidad y gravedad, reclamen públicamente la comisión de acciones violentas por parte de organizaciones o grupos terroristas.

Artículo 171.

1. Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior.

2. Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere.

3. Si el hecho descrito en el apartado anterior consistiere en la amenaza de revelar o denunciar la comisión de algún delito el ministerio fiscal podrá, para facilitar el castigo de la amenaza, abstenerse de acusar por el delito cuya revelación se hubiere amenazado, salvo que éste estuviere castigado con pena de prisión superior a dos años. En este último caso, el juez o tribunal podrá rebajar la sanción en uno o dos grados.

4. El que de modo leve amenace a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, será castigado con la pena de prisión de seis meses a un año o de trabajos en beneficio de la

comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de un año y un día a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento hasta cinco años.

Igual pena se impondrá al que de modo leve amenace a una persona especialmente vulnerable que conviva con el autor.

5. El que de modo leve amenace con armas u otros instrumentos peligrosos a alguna de las personas a las que se refiere el artículo 173.2, exceptuadas las contempladas en el apartado anterior de este artículo, será castigado con la pena de prisión de tres meses a un año o trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de uno a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento por tiempo de seis meses a tres años.

Se impondrán las penas previstas en los apartados 4 y 5, en su mitad superior cuando el delito se perpetre en presencia de menores, o tenga lugar en el domicilio común o en el domicilio de la víctima, o se realice quebrantando una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza.

6. No obstante lo previsto en los apartados 4 y 5, el Juez o Tribunal, razonándolo en sentencia, en atención a las circunstancias personales del autor y a las concurrentes en la realización del hecho, podrá imponer la pena inferior en grado.

7. Fuera de los casos anteriores, el que de modo leve amenace a otro será castigado con la pena de multa de uno a tres meses. Este hecho sólo será perseguible mediante denuncia de la persona agraviada o de su representante legal.

Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, la pena será la de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, ésta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84. En estos casos no será exigible la denuncia a que se refiere el párrafo anterior.

CAPÍTULO III

De las coacciones

Artículo 172.

1. El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados.

Cuando la coacción ejercida tuviera como objeto impedir el ejercicio de un derecho fundamental se le impondrán las penas en su mitad superior, salvo que el hecho tuviera señalada mayor pena en otro precepto de este Código.

También se impondrán las penas en su mitad superior cuando la coacción ejercida tuviera por objeto impedir el legítimo disfrute de la vivienda.

2. El que de modo leve coaccione a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad, aun sin convivencia, será castigado con la pena de prisión de seis meses a un año o de trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de un año y un día a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento hasta cinco años.

Igual pena se impondrá al que de modo leve coaccione a una persona especialmente vulnerable que conviva con el autor.

Se impondrá la pena en su mitad superior cuando el delito se perpetre en presencia de menores, o tenga lugar en el domicilio común o en el domicilio de la víctima, o se realice quebrantando una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza.

No obstante lo previsto en los párrafos anteriores, el Juez o Tribunal, razonándolo en sentencia, en atención a las circunstancias personales del autor y a las concurrentes en la realización del hecho, podrá imponer la pena inferior en grado.

3. Fuera de los casos anteriores, el que cause a otro una coacción de carácter leve, será castigado con la pena de multa de uno a tres meses. Este hecho sólo será perseguible mediante denuncia de la persona agraviada o de su representante legal.

Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, la pena será la de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, ésta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84. En estos casos no será exigible la denuncia a que se refiere el párrafo anterior.

Artículo 172 bis.

1. El que con intimidación grave o violencia compeliere a otra persona a contraer matrimonio será castigado con una pena de prisión de seis meses a tres años y seis meses o con multa de doce a veinticuatro meses, según la gravedad de la coacción o de los medios empleados.

2. La misma pena se impondrá a quien, con la finalidad de cometer los hechos a que se refiere el apartado anterior, utilice violencia, intimidación grave o engaño para forzar a otro a abandonar el territorio español o a no regresar al mismo.

3. Las penas se impondrán en su mitad superior cuando la víctima fuera menor de edad.

Artículo 172 ter.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

[. . .]

CAPÍTULO IV

De los delitos de exhibicionismo y provocación sexual

Artículo 185.

El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

Artículo 186.

El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

CAPÍTULO V

De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.

Artículo 187.

1. El que, empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima, determine a una persona mayor de edad a ejercer o a mantenerse en la prostitución, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses.

Se impondrá la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses a quien se lucre explotando la prostitución de otra persona, aun con el consentimiento de la misma. En todo caso, se entenderá que hay explotación cuando concurra alguna de las siguientes circunstancias:

a) Que la víctima se encuentre en una situación de vulnerabilidad personal o económica.

b) Que se le impongan para su ejercicio condiciones gravosas, desproporcionadas o abusivas.

2. Se impondrán las penas previstas en los apartados anteriores en su mitad superior, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:

a) Cuando el culpable se hubiera prevalido de su condición de autoridad, agente de ésta o funcionario público. En este caso se aplicará, además, la pena de inhabilitación absoluta de seis a doce años.

b) Cuando el culpable perteneciere a una organización o grupo criminal que se dedicare a la realización de tales actividades.

c) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

3. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las agresiones o abusos sexuales cometidos sobre la persona prostituida.

Artículo 188.

1. El que induzca, promueva, favorezca o facilite la prostitución de un menor de edad o una persona con discapacidad necesitada de especial protección, o se lucre con ello, o explote de algún otro modo a un menor o a una persona con discapacidad para estos fines, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses.

Si la víctima fuera menor de dieciséis años, se impondrá la pena de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

2. Si los hechos descritos en el apartado anterior se cometieran con violencia o intimidación, además de las penas de multa previstas, se impondrá la pena de prisión de

cinco a diez años si la víctima es menor de dieciséis años, y la pena de prisión de cuatro a seis años en los demás casos.

3. Se impondrán las penas superiores en grado a las previstas en los apartados anteriores, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:

a) Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad, discapacidad o situación.

b) Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, descendiente o hermano, por naturaleza o adopción, o afines, con la víctima.

c) Cuando, para la ejecución del delito, el responsable se hubiera prevalido de su condición de autoridad, agente de ésta o funcionario público. En este caso se impondrá, además, una pena de inhabilitación absoluta de seis a doce años.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando los hechos se hubieren cometido por la actuación conjunta de dos o más personas.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

4. El que solicite, acepte u obtenga, a cambio de una remuneración o promesa, una relación sexual con una persona menor de edad o una persona con discapacidad necesitada de especial protección, será castigado con una pena de uno a cuatro años de prisión. Si el menor no hubiera cumplido dieciséis años de edad, se impondrá una pena de dos a seis años de prisión.

5. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las infracciones contra la libertad o indemnidad sexual cometidas sobre los menores y personas con discapacidad necesitadas de especial protección.

Artículo 189.

1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.

b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio.

c) Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando el material pornográfico fuera de notoria importancia.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.

h) Cuando concurra la agravante de reincidencia.

3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

Artículo 189 bis.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este Capítulo, se le impondrán las siguientes penas:

a) Multa del triple al quíntuple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.

b) Multa del doble al cuádruple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años no incluida en el anterior inciso.

c) Multa del doble al triple del beneficio obtenido, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 190.

La condena de un Juez o Tribunal extranjero, impuesta por delitos comprendidos en este capítulo, será equiparada a las sentencias de los Jueces o Tribunales españoles a los efectos de la aplicación de la circunstancia agravante de reincidencia.

[. . .]

TÍTULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO I

Del descubrimiento y revelación de secretos

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 quater.

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Artículo 197 quinquies.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 198.

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199.

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200.

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Artículo 201.

1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130.

[. . .]

TÍTULO XI

Delitos contra el honor

CAPÍTULO I

De la calumnia

Artículo 205.

Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 206.

Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses.

Artículo 207.

El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado.

CAPÍTULO II

De la injuria

Artículo 208.

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado 4 del artículo 173.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 209.

Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses.

Artículo 210.

El acusado de injuria quedará exento de responsabilidad probando la verdad de las imputaciones cuando estas se dirijan contra funcionarios públicos sobre hechos concernientes al ejercicio de sus cargos o referidos a la comisión de infracciones administrativas.

CAPÍTULO III

Disposiciones generales

Artículo 211.

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212.

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 213.

Si la calumnia o injuria fueren cometidas mediante precio, recompensa o promesa, los Tribunales impondrán, además de las penas señaladas para los delitos de que se trate, la de inhabilitación especial prevista en los artículos 42 ó 45 del presente Código, por tiempo de seis meses a dos años.

Artículo 214.

Si el acusado de calumnia o injuria reconociere ante la autoridad judicial la falsedad o falta de certeza de las imputaciones y se retractare de ellas, el Juez o Tribunal impondrá la pena inmediatamente inferior en grado y podrá dejar de imponer la pena de inhabilitación que establece el artículo anterior.

El Juez o Tribunal ante quien se produjera el reconocimiento ordenará que se entregue testimonio de retractación al ofendido y, si éste lo solicita, ordenará su publicación en el mismo medio en que se vertió la calumnia o injuria, en espacio idéntico o similar a aquél en que se produjo su difusión y dentro del plazo que señale el Juez o Tribunal sentenciador.

Artículo 215.

1. Nadie será penado por calumnia o injuria sino en virtud de querella de la persona ofendida por el delito o de su representante legal. Se procederá de oficio cuando la ofensa se dirija contra funcionario público, autoridad o agente de la misma sobre hechos concernientes al ejercicio de sus cargos.

2. Nadie podrá deducir acción de calumnia o injuria vertidas en juicio sin previa licencia del Juez o Tribunal que de él conociere o hubiere conocido.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130 de este Código.

Artículo 216.

En los delitos de calumnia o injuria se considera que la reparación del daño comprende también la publicación o divulgación de la sentencia condenatoria, a costa del condenado por tales delitos, en el tiempo y forma que el Juez o Tribunal consideren más adecuado a tal fin, oídas las dos partes.

[. . .]

Sección 1.ª De las estafas

Artículo 248.

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Artículo 249.

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.

Artículo 250.

1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:

1.º Recaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.

2.º Se perpetre abusando de firma de otro, o sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, protocolo o documento público u oficial de cualquier clase.

3.º Recaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.

4.º Revista especial gravedad, atendiendo a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia.

5.º El valor de la defraudación supere los 50.000 euros, o afecte a un elevado número de personas.

6.º Se cometa con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional.

7.º Se cometa estafa procesal. Incurren en la misma los que, en un procedimiento judicial de cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero.

8.º Al delinquir el culpable hubiera sido condenado ejecutoriamente al menos por tres delitos comprendidos en este Capítulo. No se tendrán en cuenta antecedentes cancelados o que debieran serlo.

2. Si concurrieran las circunstancias incluidas en los numerales 4.º, 5.º, 6.º o 7.º con la del numeral 1.º del apartado anterior, se impondrán las penas de prisión de cuatro a ocho años y multa de doce a veinticuatro meses. La misma pena se impondrá cuando el valor de la defraudación supere los 250.000 euros.

Artículo 251.

Será castigado con la pena de prisión de uno a cuatro años:

1.º Quien, atribuyéndose falsamente sobre una cosa mueble o inmueble facultad de disposición de la que carece, bien por no haberla tenido nunca, bien por haberla ya ejercitado, la enajenare, gravare o arrendare a otro, en perjuicio de éste o de tercero.

2.º El que dispusiere de una cosa mueble o inmueble ocultando la existencia de cualquier carga sobre la misma, o el que, habiéndola enajenado como libre, la gravare o enajenare nuevamente antes de la definitiva transmisión al adquirente, en perjuicio de éste, o de un tercero.

3.º El que otorgare en perjuicio de otro un contrato simulado.

Artículo 251 bis.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en esta Sección, se le impondrán las siguientes penas:

a) Multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.

b) Multa del doble al cuádruple de la cantidad defraudada, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

[. . .]

Artículo 263.

1. El que causare daños en propiedad ajena no comprendidos en otros títulos de este Código, será castigado con multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño.

Si la cuantía del daño causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

2. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el apartado anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o como consecuencia de acciones ejecutadas en el ejercicio de sus funciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2.º Que se cause por cualquier medio, infección o contagio de ganado.

3.º Que se empleen sustancias venenosas o corrosivas.

4.º Que afecten a bienes de dominio o uso público o comunal.

5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

6.º Se hayan ocasionado daños de especial gravedad o afectado a los intereses generales.

Artículo 264.

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 bis.

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 264 quater.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:

a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.

b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 265.

El que destruyere, dañare de modo grave, o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad, será castigado con la pena de prisión de dos a cuatro años si el daño causado excediere de mil euros.

Artículo 266.

1. Será castigado con la pena de prisión de uno a tres años el que cometiere los daños previstos en el apartado 1 del artículo 263 mediante incendio, o provocando explosiones, o utilizando cualquier otro medio de similar potencia destructiva o que genere un riesgo relevante de explosión o de causación de otros daños de especial gravedad, o poniendo en peligro la vida o la integridad de las personas.

2. Será castigado con la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses el que cometiere los daños previstos en el apartado 2 del artículo 263, en cualquiera de las circunstancias mencionadas en el apartado anterior.

3. Será castigado con la pena de prisión de cuatro a ocho años el que cometiere los daños previstos en los artículos 265, 323 y 560, en cualquiera de las circunstancias mencionadas en el apartado 1 del presente artículo.

4. En cualquiera de los supuestos previstos en los apartados anteriores, cuando se cometieren los daños concurriendo la provocación de explosiones o la utilización de otros medios de similar potencia destructiva y, además, se pusiera en peligro la vida o integridad de las personas, la pena se impondrá en su mitad superior.

En caso de incendio será de aplicación lo dispuesto en el artículo 351.

Artículo 267.

Los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos.

Las infracciones a que se refiere este artículo sólo serán perseguibles previa denuncia de la persona agraviada o de su representante legal. El Ministerio Fiscal también podrá denunciar cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida.

En estos casos, el perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130 de este Código.

CAPÍTULO X

Disposiciones comunes a los capítulos anteriores

Artículo 268.

1. Están exentos de responsabilidad criminal y sujetos únicamente a la civil los cónyuges que no estuvieren separados legalmente o de hecho o en proceso judicial de separación, divorcio o nulidad de su matrimonio y los ascendientes, descendientes y hermanos por naturaleza o por adopción, así como los afines en primer grado si viviesen juntos, por los delitos patrimoniales que se causaren entre sí, siempre que no concurra violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad.

2. Esta disposición no es aplicable a los extraños que participaren en el delito.

Artículo 269.

La provocación, la conspiración y la proposición para cometer los delitos de robo, extorsión, estafa o apropiación indebida, serán castigadas con la pena inferior en uno o dos grados a la del delito correspondiente.

CAPÍTULO XI

De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores

Sección 1.ª De los delitos relativos a la propiedad intelectual

Artículo 270.

1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

3. En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.

Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.

4. En los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

5. Serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes:

a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente.

b) Importen intencionadamente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.

c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización.

d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.

6. Será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo.

Artículo 271.

Se impondrá la pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando se cometa el delito del artículo anterior concurriendo alguna de las siguientes circunstancias:

a) Que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica.

b) Que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente, el número de obras, o de la transformación, ejecución o interpretación de las mismas, ilícitamente reproducidas, distribuidas, comunicadas al público o puestas a su disposición, o a la especial importancia de los perjuicios ocasionados.

c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual.

d) Que se utilice a menores de 18 años para cometer estos delitos.

Artículo 272.

1. La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios.

2. En el supuesto de sentencia condenatoria, el Juez o Tribunal podrá decretar la publicación de ésta, a costa del infractor, en un periódico oficial.

Sección 2.ª De los delitos relativos a la propiedad industrial

Artículo 273.

1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.

2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.

3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor.

Artículo 274.

1. Será castigado con las penas de uno a cuatro años de prisión y multa de doce a veinticuatro meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro,

a) fabrique, produzca o importe productos que incorporen un signo distintivo idéntico o confundible con aquel, u

b) ofrezca, distribuya, o comercialice al por mayor productos que incorporen un signo distintivo idéntico o confundible con aquel, o los almacene con esa finalidad, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

2. Será castigado con las penas de seis meses a tres años de prisión el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, ofrezca, distribuya o comercialice al por menor, o preste servicios o desarrolle actividades, que incorporen un signo distintivo idéntico o confundible con aquél, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

La misma pena se impondrá a quien reproduzca o imite un signo distintivo idéntico o confundible con aquél para su utilización para la comisión de las conductas sancionadas en este artículo.

3. La venta ambulante u ocasional de los productos a que se refieren los apartados anteriores será castigada con la pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 276, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

4. Será castigado con las penas de uno a tres años de prisión el que, con fines agrarios o comerciales, sin consentimiento del titular de un título de obtención vegetal y con conocimiento de su registro, produzca o reproduzca, acondicione con vistas a la producción o reproducción, ofrezca en venta, venda o comercialice de otra forma, exporte o importe, o posea para cualquiera de los fines mencionados, material vegetal de reproducción o multiplicación de una variedad vegetal protegida conforme a la legislación nacional o de la Unión Europea sobre protección de obtenciones vegetales.

Será castigado con la misma pena quien realice cualesquiera de los actos descritos en el párrafo anterior utilizando, bajo la denominación de una variedad vegetal protegida, material vegetal de reproducción o multiplicación que no pertenezca a tal variedad.

Artículo 275.

Las mismas penas previstas en el artículo anterior se impondrán a quien intencionadamente y sin estar autorizado para ello, utilice en el tráfico económico una denominación de origen o una indicación geográfica representativa de una calidad determinada legalmente protegidas para distinguir los productos amparados por ellas, con conocimiento de esta protección.

Artículo 276.

Se impondrá la pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica.

b) Que los hechos revistan especial gravedad, atendiendo al valor de los objetos producidos ilícitamente, distribuidos, comercializados u ofrecidos, o a la especial importancia de los perjuicios ocasionados.

c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad industrial.

d) Que se utilice a menores de 18 años para cometer estos delitos.

Artículo 277.

Será castigado con las penas de prisión de seis meses a dos años y multa de seis a veinticuatro meses, el que intencionadamente haya divulgado la invención objeto de una solicitud de patente secreta, en contravención con lo dispuesto en la legislación de patentes, siempre que ello sea en perjuicio de la defensa nacional.

Sección 3.ª De los delitos relativos al mercado y a los consumidores

Artículo 278.

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 279.

La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior.

Artículo 280.

El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses.

Artículo 281.

1. El que detrajere del mercado materias primas o productos de primera necesidad con la intención de desabastecer un sector del mismo, de forzar una alteración de precios, o de perjudicar gravemente a los consumidores, será castigado con la pena de prisión de uno a cinco años y multa de doce a veinticuatro meses.

2. Se impondrá la pena superior en grado si el hecho se realiza en situaciones de grave necesidad o catastróficas.

Artículo 282.

Serán castigados con la pena de prisión de seis meses a un año o multa de 12 a 24 meses los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

Artículo 282 bis.

Los que, como administradores de hecho o de derecho de una sociedad emisora de valores negociados en los mercados de valores, falsearan la información económico-financiera contenida en los folletos de emisión de cualesquiera instrumentos financieros o las informaciones que la sociedad debe publicar y difundir conforme a la legislación del mercado de valores sobre sus recursos, actividades y negocios presentes y futuros, con el propósito de captar inversores o depositantes, colocar cualquier tipo de activo financiero, u obtener financiación por cualquier medio, serán castigados con la pena de prisión de uno a cuatro años, sin perjuicio de lo dispuesto en el artículo 308 de este Código.

En el supuesto de que se llegue a obtener la inversión, el depósito, la colocación del activo o la financiación, con perjuicio para el inversor, depositante, adquiriente de los activos financieros o acreedor, se impondrá la pena en la mitad superior. Si el perjuicio causado fuera de notoria gravedad, la pena a imponer será de uno a seis años de prisión y multa de seis a doce meses.

Artículo 283.

Se impondrán las penas de prisión de seis meses a un año y multa de seis a dieciocho meses a los que, en perjuicio del consumidor, facturen cantidades superiores por productos o servicios cuyo costo o precio se mida por aparatos automáticos, mediante la alteración o manipulación de éstos.

Artículo 284.

Se impondrá la pena de prisión de seis meses a dos años o multa de doce a veinticuatro meses a los que:

1.º Empleando violencia, amenaza o engaño, intentaren alterar los precios que hubieren de resultar de la libre concurrencia de productos, mercancías, títulos valores o instrumentos

financieros, servicios o cualesquiera otras cosas muebles o inmuebles que sean objeto de contratación, sin perjuicio de la pena que pudiere corresponderles por otros delitos cometidos.

2.º Difundieren noticias o rumores, por sí o a través de un medio de comunicación, sobre personas o empresas en que a sabiendas se ofrecieren datos económicos total o parcialmente falsos con el fin de alterar o preservar el precio de cotización de un valor o instrumento financiero, obteniendo para sí o para tercero un beneficio económico superior a los 300.000 euros o causando un perjuicio de idéntica cantidad.

3.º Utilizando información privilegiada, realizaren transacciones o dieren órdenes de operación susceptibles de proporcionar indicios engañosos sobre la oferta, la demanda o el precio de valores o instrumentos financieros, o se aseguraren utilizando la misma información, por sí o en concierto con otros, una posición dominante en el mercado de dichos valores o instrumentos con la finalidad de fijar sus precios en niveles anormales o artificiales.

En todo caso se impondrá la pena de inhabilitación de uno a dos años para intervenir en el mercado financiero como actor, agente o mediador o informador.

Artículo 285.

1. Quien de forma directa o por persona interpuesta usare de alguna información relevante para la cotización de cualquier clase de valores o instrumentos negociados en algún mercado organizado, oficial o reconocido, a la que haya tenido acceso reservado con ocasión del ejercicio de su actividad profesional o empresarial, o la suministrare obteniendo para sí o para un tercero un beneficio económico superior a 600.000 euros o causando un perjuicio de idéntica cantidad, será castigado con la pena de prisión de uno a cuatro años, multa del tanto al triplo del beneficio obtenido o favorecido e inhabilitación especial para el ejercicio de la profesión o actividad de dos a cinco años.

2. Se aplicará la pena de prisión de cuatro a seis años, la multa del tanto al triplo del beneficio obtenido o favorecido e inhabilitación especial para el ejercicio de la profesión o actividad de dos a cinco años, cuando en las conductas descritas en el apartado anterior concurra alguna de las siguientes circunstancias:

1.ª Que los sujetos se dediquen de forma habitual a tales prácticas abusivas.
2.ª Que el beneficio obtenido sea de notoria importancia.
3.ª Que se cause grave daño a los intereses generales.

Artículo 286.

1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

3. A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.

4. A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación.

Sección 4.ª Delitos de corrupción en los negocios

Artículo 286 bis.

1. El directivo, administrador, empleado o colaborador de una empresa mercantil o de una sociedad que, por sí o por persona interpuesta, reciba, solicite o acepte un beneficio o ventaja no justificados de cualquier naturaleza, para sí o para un tercero, como contraprestación para favorecer indebidamente a otro en la adquisición o venta de mercancías, o en la contratación de servicios o en las relaciones comerciales, será castigado con la pena de prisión de seis meses a cuatro años, inhabilitación especial para el ejercicio de industria o comercio por tiempo de uno a seis años y multa del tanto al triplo del valor del beneficio o ventaja.

2. Con las mismas penas será castigado quien, por sí o por persona interpuesta, prometa, ofrezca o conceda a directivos, administradores, empleados o colaboradores de una empresa mercantil o de una sociedad, un beneficio o ventaja no justificados, de cualquier naturaleza, para ellos o para terceros, como contraprestación para que le favorezca indebidamente a él o a un tercero frente a otros en la adquisición o venta de mercancías, contratación de servicios o en las relaciones comerciales.

3. Los jueces y tribunales, en atención a la cuantía del beneficio o al valor de la ventaja, y a la trascendencia de las funciones del culpable, podrán imponer la pena inferior en grado y reducir la de multa a su prudente arbitrio.

4. Lo dispuesto en este artículo será aplicable, en sus respectivos casos, a los directivos, administradores, empleados o colaboradores de una entidad deportiva, cualquiera que sea la forma jurídica de ésta, así como a los deportistas, árbitros o jueces, respecto de aquellas conductas que tengan por finalidad predeterminar o alterar de manera deliberada y fraudulenta el resultado de una prueba, encuentro o competición deportiva de especial relevancia económica o deportiva.

A estos efectos, se considerará competición deportiva de especial relevancia económica, aquélla en la que la mayor parte de los participantes en la misma perciban cualquier tipo de retribución, compensación o ingreso económico por su participación en la actividad; y competición deportiva de especial relevancia deportiva, la que sea calificada en el calendario deportivo anual aprobado por la federación deportiva correspondiente como competición oficial de la máxima categoría de la modalidad, especialidad, o disciplina de que se trate.

5. A los efectos de este artículo resulta aplicable lo dispuesto en el artículo 297.

Artículo 286 ter.

1. Los que mediante el ofrecimiento, promesa o concesión de cualquier beneficio o ventaja indebidos, pecuniarios o de otra clase, corrompieren o intentaren corromper, por sí o por persona interpuesta, a una autoridad o funcionario público en beneficio de estos o de un tercero, o atendieran sus solicitudes al respecto, con el fin de que actúen o se abstengan de actuar en relación con el ejercicio de funciones públicas para conseguir o conservar un contrato, negocio o cualquier otra ventaja competitiva en la realización de actividades económicas internacionales, serán castigados, salvo que ya lo estuvieran con una pena más grave en otro precepto de este Código, con las penas de prisión de prisión de tres a seis años, multa de doce a veinticuatro meses, salvo que el beneficio obtenido fuese superior a la cantidad resultante, en cuyo caso la multa será del tanto al triplo del montante de dicho beneficio.

Además de las penas señaladas, se impondrá en todo caso al responsable la pena de prohibición de contratar con el sector público, así como la pérdida de la posibilidad de obtener subvenciones o ayudas públicas y del derecho a gozar de beneficios o incentivos fiscales y de la Seguridad Social, y la prohibición de intervenir en transacciones comerciales de trascendencia pública por un periodo de siete a doce años.

2. A los efectos de este artículo se entenderá por funcionario público los determinados por los artículos 24 y 427.

Artículo 286 quater.

1. Si los hechos a que se refieren los artículos de esta Sección resultaran de especial gravedad, se impondrá la pena en su mitad superior, pudiéndose llegar hasta la superior en grado.

Los hechos se considerarán, en todo caso, de especial gravedad cuando:

a) el beneficio o ventaja tenga un valor especialmente elevado,

b) la acción del autor no sea meramente ocasional,

c) se trate de hechos cometidos en el seno de una organización o grupo criminal, o

d) el objeto del negocio versara sobre bienes o servicios humanitarios o cualesquiera otros de primera necesidad.

En el caso del apartado 4 del artículo 286 bis, los hechos se considerarán también de especial gravedad cuando:

a) tengan como finalidad influir en el desarrollo de juegos de azar o apuestas; o

b) sean cometidos en una competición deportiva oficial de ámbito estatal calificada como profesional o en una competición deportiva internacional.

[. . .]

TÍTULO XVIII

De las falsedades

[. . .]

CAPÍTULO IV

De la usurpación del estado civil

Artículo 401.

El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

[. . .]

CAPÍTULO III

Del descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional

Artículo 598.

El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con la pena de prisión de uno a cuatro años.

Artículo 599.

La pena establecida en el artículo anterior se aplicará en su mitad superior cuando concurra alguna de las circunstancias siguientes:

1.º Que el sujeto activo sea depositario o conocedor del secreto o información por razón de su cargo o destino.

2.º Que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión.

Artículo 600.

1. El que sin autorización expresa reprodujere planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento esté protegido y reservado por una información legalmente calificada como reservada o secreta, será castigado con la pena de prisión de seis meses a tres años.

2. Con la misma pena será castigado el que tenga en su poder objetos o información legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional, sin cumplir las disposiciones establecidas en la legislación vigente.

Artículo 601.

El que, por razón de su cargo, comisión o servicio, tenga en su poder o conozca oficialmente objetos o información legalmente calificada como reservada o secreta o de interés militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave dé lugar a que sean conocidos por persona no autorizada o divulgados, publicados o inutilizados, será castigado con la pena de prisión de seis meses a un año.

Artículo 602.

El que descubriere, violare, revelare, sustrajere o utilizare información legalmente calificada como reservada o secreta relacionada con la energía nuclear, será castigado con la pena de prisión de seis meses a tres años, salvo que el hecho tenga señalada pena más grave en otra Ley.

Artículo 603.

El que destruyere, inutilizare, falseare o abriere sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o destino, será castigado con la pena de prisión de dos a cinco años e inhabilitación especial de empleo o cargo público por tiempo de tres a seis años.

§ 39

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 11, de 13 de enero de 2000
Última modificación: 28 de diciembre de 2012
Referencia: BOE-A-2000-641

[. . .]

TÍTULO PRELIMINAR

Artículo 1. *Declaración general.*

1. Esta Ley se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales.

2. Las personas a las que se aplique la presente Ley gozarán de todos los derechos reconocidos en la Constitución y en el ordenamiento jurídico, particularmente en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, así como en la Convención sobre los Derechos del Niño de 20 de noviembre de 1989 y en todas aquellas normas sobre protección de menores contenidas en los Tratados válidamente celebrados por España.

TÍTULO I

Del ámbito de aplicación de la Ley

Artículo 2. *Competencia de los Jueces de Menores.*

1. Los Jueces de Menores serán competentes para conocer de los hechos cometidos por las personas mencionadas en el artículo 1 de esta Ley, así como para hacer ejecutar las sentencias, sin perjuicio de las facultades atribuidas por esta Ley a las Comunidades Autónomas respecto a la protección y reforma de menores.

2. Los Jueces de Menores serán asimismo competentes para resolver sobre las responsabilidades civiles derivadas de los hechos cometidos por las personas a las que resulta aplicable la presente Ley.

3. La competencia corresponde al Juez de Menores del lugar donde se haya cometido el hecho delictivo, sin perjuicio de lo establecido en el artículo 20.3 de esta Ley.

4. La competencia para conocer de los delitos previstos en los artículos 571 a 580 del Código Penal corresponderá al Juzgado Central de Menores de la Audiencia Nacional.

Corresponderá igualmente al Juzgado Central de Menores de la Audiencia Nacional la competencia para conocer de los delitos cometidos por menores en el extranjero cuando conforme al artículo 23 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y a los Tratados Internacionales corresponda su conocimiento a la jurisdicción española.

La referencia del último inciso del apartado 4 del artículo 17 y cuantas otras se contienen en la presente Ley al Juez de Menores se entenderán hechas al Juez Central de Menores en lo que afecta a los menores imputados por cualquiera de los delitos a que se refieren los dos párrafos anteriores.

Artículo 3. *Régimen de los menores de catorce años.*

Cuando el autor de los hechos mencionados en los artículos anteriores sea menor de catorce años, no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes. El Ministerio Fiscal deberá remitir a la entidad pública de protección de menores testimonio de los particulares que considere precisos respecto al menor, a fin de valorar su situación, y dicha entidad habrá de promover las medidas de protección adecuadas a las circunstancias de aquél conforme a lo dispuesto en la Ley Orgánica 1/1996, de 15 de enero.

Artículo 4. *Derechos de las víctimas y de los perjudicados.*

El Ministerio Fiscal y el Juez de Menores velarán en todo momento por la protección de los derechos de las víctimas y de los perjudicados por las infracciones cometidas por los menores.

De manera inmediata se les instruirá de las medidas de asistencia a las víctimas que prevé la legislación vigente.

Las víctimas y los perjudicados tendrán derecho a personarse y ser parte en el expediente que se incoe al efecto, para lo cual el secretario judicial les informará en los términos previstos en los artículos 109 y 110 de la Ley de Enjuiciamiento Criminal, instruyéndoles de su derecho a nombrar abogado o instar el nombramiento de abogado de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita. Asimismo, les informará de que, de no personarse en el expediente y no hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere.

Los que se personaren podrán desde entonces tomar conocimiento de lo actuado e instar la práctica de diligencias y cuanto a su derecho convenga. Sin perjuicio de lo anterior, el secretario judicial deberá comunicar a las víctimas y perjudicados, se hayan o no personado, todas aquellas resoluciones que se adopten tanto por el Ministerio Fiscal como por el Juez de Menores, que puedan afectar a sus intereses.

En especial, cuando el Ministerio Fiscal, en aplicación de lo dispuesto en el artículo 18 de esta Ley, desista de la incoación del expediente deberá inmediatamente ponerlo en conocimiento de las víctimas y perjudicados haciéndoles saber su derecho a ejercitar las acciones civiles que les asisten ante la jurisdicción civil.

Del mismo modo, el secretario judicial notificará por escrito la sentencia que se dicte a las víctimas y perjudicados por la infracción penal, aunque no se hayan mostrado parte en el expediente.

Artículo 5. *Bases de la responsabilidad de los menores.*

1. Los menores serán responsables con arreglo a esta Ley cuando hayan cometido los hechos a los que se refiere el artículo 1 y no concurra en ellos ninguna de las causas de exención o extinción de la responsabilidad criminal previstas en el vigente Código Penal.

2. No obstante lo anterior, a los menores en quienes concurran las circunstancias previstas en los números 1.º, 2.º y 3.º del artículo 20 del vigente Código Penal les serán aplicables, en caso necesario, las medidas terapéuticas a las que se refiere el artículo 7.1, letras d) y e), de la presente Ley.

3. Las edades indicadas en el articulado de esta Ley se han de entender siempre referidas al momento de la comisión de los hechos, sin que el haberse rebasado las mismas antes del comienzo del procedimiento o durante la tramitación del mismo tenga incidencia alguna sobre la competencia atribuida por esta misma Ley a los Jueces y Fiscales de Menores.

Artículo 6. *De la intervención del Ministerio Fiscal.*

Corresponde al Ministerio Fiscal la defensa de los derechos que a los menores reconocen las leyes, así como la vigilancia de las actuaciones que deban efectuarse en su interés y la observancia de las garantías del procedimiento, para lo cual dirigirá personalmente la investigación de los hechos y ordenará que la policía judicial practique las actuaciones necesarias para la comprobación de aquéllos y de la participación del menor en los mismos, impulsando el procedimiento.

TÍTULO II

De las medidas

Artículo 7. *Definición de las medidas susceptibles de ser impuestas a los menores y reglas generales de determinación de las mismas.*

1. Las medidas que pueden imponer los Jueces de Menores, ordenadas según la restricción de derechos que suponen, son las siguientes:

a) Internamiento en régimen cerrado. Las personas sometidas a esta medida residirán en el centro y desarrollarán en el mismo las actividades formativas, educativas, laborales y de ocio.

b) Internamiento en régimen semiabierto. Las personas sometidas a esta medida residirán en el centro, pero podrán realizar fuera del mismo alguna o algunas de las actividades formativas, educativas, laborales y de ocio establecidas en el programa individualizado de ejecución de la medida. La realización de actividades fuera del centro quedará condicionada a la evolución de la persona y al cumplimiento de los objetivos previstos en las mismas, pudiendo el Juez de Menores suspenderlas por tiempo determinado, acordando que todas las actividades se lleven a cabo dentro del centro.

c) Internamiento en régimen abierto. Las personas sometidas a esta medida llevarán a cabo todas las actividades del proyecto educativo en los servicios normalizados del entorno, residiendo en el centro como domicilio habitual, con sujeción al programa y régimen interno del mismo.

d) Internamiento terapéutico en régimen cerrado, semiabierto o abierto. En los centros de esta naturaleza se realizará una atención educativa especializada o tratamiento específico dirigido a personas que padezcan anomalías o alteraciones psíquicas, un estado de dependencia de bebidas alcohólicas, drogas tóxicas o sustancias psicotrópicas, o alteraciones en la percepción que determinen una alteración grave de la conciencia de la realidad. Esta medida podrá aplicarse sola o como complemento de otra medida prevista en este artículo. Cuando el interesado rechace un tratamiento de deshabituación, el Juez habrá de aplicarle otra medida adecuada a sus circunstancias.

e) Tratamiento ambulatorio. Las personas sometidas a esta medida habrán de asistir al centro designado con la periodicidad requerida por los facultativos que las atiendan y seguir las pautas fijadas para el adecuado tratamiento de la anomalía o alteración psíquica, adicción al consumo de bebidas alcohólicas, drogas tóxicas o sustancias psicotrópicas, o alteraciones en la percepción que padezcan. Esta medida podrá aplicarse sola o como complemento de otra medida prevista en este artículo. Cuando el interesado rechace un tratamiento de deshabituación, el Juez habrá de aplicarle otra medida adecuada a sus circunstancias.

f) Asistencia a un centro de día. Las personas sometidas a esta medida residirán en su domicilio habitual y acudirán a un centro, plenamente integrado en la comunidad, a realizar actividades de apoyo, educativas, formativas, laborales o de ocio.

g) Permanencia de fin de semana. Las personas sometidas a esta medida permanecerán en su domicilio o en un centro hasta un máximo de treinta y seis horas entre la tarde o noche del viernes y la noche del domingo, a excepción, en su caso, del tiempo que deban dedicar a las tareas socio-educativas asignadas por el Juez que deban llevarse a cabo fuera del lugar de permanencia.

h) Libertad vigilada. En esta medida se ha de hacer un seguimiento de la actividad de la persona sometida a la misma y de su asistencia a la escuela, al centro de formación profesional o al lugar de trabajo, según los casos, procurando ayudar a aquélla a superar los factores que determinaron la infracción cometida. Asimismo, esta medida obliga, en su caso, a seguir las pautas socio-educativas que señale la entidad pública o el profesional encargado de su seguimiento, de acuerdo con el programa de intervención elaborado al efecto y aprobado por el Juez de Menores. La persona sometida a la medida también queda obligada a mantener con dicho profesional las entrevistas establecidas en el programa y a cumplir, en su caso, las reglas de conducta impuestas por el Juez, que podrán ser alguna o algunas de las siguientes:

1.ª Obligación de asistir con regularidad al centro docente correspondiente, si el menor está en edad de escolarización obligatoria, y acreditar ante el Juez dicha asistencia regular o justificar en su caso las ausencias, cuantas veces fuere requerido para ello.

2.ª Obligación de someterse a programas de tipo formativo, cultural, educativo, profesional, laboral, de educación sexual, de educación vial u otros similares.

3.ª Prohibición de acudir a determinados lugares, establecimientos o espectáculos.

4.ª Prohibición de ausentarse del lugar de residencia sin autorización judicial previa.

5.ª Obligación de residir en un lugar determinado.

6.ª Obligación de comparecer personalmente ante el Juzgado de Menores o profesional que se designe, para informar de las actividades realizadas y justificarlas.

7.ª Cualesquiera otras obligaciones que el Juez, de oficio o a instancia del Ministerio Fiscal, estime convenientes para la reinserción social del sentenciado, siempre que no atenten contra su dignidad como persona. Si alguna de estas obligaciones implicase la imposibilidad del menor de continuar conviviendo con sus padres, tutores o guardadores, el Ministerio Fiscal deberá remitir testimonio de los particulares a la entidad pública de protección del menor, y dicha entidad deberá promover las medidas de protección adecuadas a las circunstancias de aquél, conforme a lo dispuesto en la Ley Orgánica 1/1996.

i) La prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez. Esta medida impedirá al menor acercarse a ellos, en cualquier lugar donde se encuentren, así como a su domicilio, a su centro docente, a sus lugares de trabajo y a cualquier otro que sea frecuentado por ellos. La prohibición de comunicarse con la víctima, o con aquellos de sus familiares u otras personas que determine el Juez o Tribunal, impedirá al menor establecer con ellas, por cualquier medio de comunicación o medio informático o telemático, contacto escrito, verbal o visual. Si esta medida implicase la imposibilidad del menor de continuar viviendo con sus padres, tutores o guardadores, el Ministerio Fiscal deberá remitir testimonio de los particulares a la entidad pública de protección del menor, y dicha entidad deberá promover las medidas de protección adecuadas a las circunstancias de aquél, conforme a lo dispuesto en la Ley Orgánica 1/1996.

j) Convivencia con otra persona, familia o grupo educativo. La persona sometida a esta medida debe convivir, durante el período de tiempo establecido por el Juez, con otra persona, con una familia distinta a la suya o con un grupo educativo, adecuadamente seleccionados para orientar a aquélla en su proceso de socialización.

k) Prestaciones en beneficio de la comunidad. La persona sometida a esta medida, que no podrá imponerse sin su consentimiento, ha de realizar las actividades no retribuidas que se le indiquen, de interés social o en beneficio de personas en situación de precariedad.

l) Realización de tareas socio-educativas. La persona sometida a esta medida ha de realizar, sin internamiento ni libertad vigilada, actividades específicas de contenido educativo encaminadas a facilitarle el desarrollo de su competencia social.

m) Amonestación. Esta medida consiste en la reprensión de la persona llevada a cabo por el Juez de Menores y dirigida a hacerle comprender la gravedad de los hechos cometidos y las consecuencias que los mismos han tenido o podrían haber tenido, instándole a no volver a cometer tales hechos en el futuro.

n) Privación del permiso de conducir ciclomotores y vehículos a motor, o del derecho a obtenerlo, o de las licencias administrativas para caza o para uso de cualquier tipo de armas. Esta medida podrá imponerse como accesoria cuando el delito o falta se hubiere cometido utilizando un ciclomotor o un vehículo a motor, o un arma, respectivamente.

ñ) Inhabilitación absoluta. La medida de inhabilitación absoluta produce la privación definitiva de todos los honores, empleos y cargos públicos sobre el que recayere, aunque sean electivos; así como la incapacidad para obtener los mismos o cualesquiera otros honores, cargos o empleos públicos, y la de ser elegido para cargo público, durante el tiempo de la medida.

2. Las medidas de internamiento constarán de dos períodos: el primero se llevará a cabo en el centro correspondiente, conforme a la descripción efectuada en el apartado anterior de este artículo, el segundo se llevará a cabo en régimen de libertad vigilada, en la modalidad elegida por el Juez. La duración total no excederá del tiempo que se expresa en los artículos 9 y 10. El equipo técnico deberá informar respecto del contenido de ambos períodos, y el Juez expresará la duración de cada uno en la sentencia.

3. Para la elección de la medida o medidas adecuadas se deberá atender de modo flexible, no sólo a la prueba y valoración jurídica de los hechos, sino especialmente a la edad, las circunstancias familiares y sociales, la personalidad y el interés del menor, puestos de manifiesto los dos últimos en los informes de los equipos técnicos y de las entidades públicas de protección y reforma de menores cuando éstas hubieran tenido conocimiento del menor por haber ejecutado una medida cautelar o definitiva con anterioridad, conforme a lo dispuesto en el artículo 27 de la presente Ley. El Juez deberá motivar en la sentencia las razones por las que aplica una determinada medida, así como el plazo de duración de la misma, a los efectos de la valoración del mencionado interés del menor.

4. El Juez podrá imponer al menor una o varias medidas de las previstas en esta Ley con independencia de que se trate de uno o más hechos, sujetándose si procede a lo dispuesto en el artículo 11 para el enjuiciamiento conjunto de varias infracciones; pero, en ningún caso, se impondrá a un menor en una misma resolución más de una medida de la misma clase, entendiendo por tal cada una de las que se enumeran en el apartado 1 de este artículo.

Artículo 8. *Principio acusatorio.*

El Juez de Menores no podrá imponer una medida que suponga una mayor restricción de derechos ni por un tiempo superior a la medida solicitada por el Ministerio Fiscal o por el acusador particular.

Tampoco podrá exceder la duración de las medidas privativas de libertad contempladas en el artículo 7.1.ª), b), c), d) y g), en ningún caso, del tiempo que hubiera durado la pena privativa de libertad que se le hubiere impuesto por el mismo hecho, si el sujeto, de haber sido mayor de edad, hubiera sido declarado responsable, de acuerdo con el Código Penal.

Artículo 9. *Régimen general de aplicación y duración de las medidas.*

No obstante lo establecido en los apartados 3 y 4 del artículo 7, la aplicación de las medidas se atendrá a las siguientes reglas:

1. Cuando los hechos cometidos sean calificados de falta, sólo se podrán imponer las medidas de libertad vigilada hasta un máximo de seis meses, amonestación, permanencia de fin de semana hasta un máximo de cuatro fines de semana, prestaciones en beneficio de la comunidad hasta cincuenta horas, privación del permiso de conducir o de otras licencias administrativas hasta un año, la prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez hasta seis meses, y la realización de tareas socio-educativas hasta seis meses.

2. La medida de internamiento en régimen cerrado sólo podrá ser aplicable cuando:

a) Los hechos estén tipificados como delito grave por el Código Penal o las leyes penales especiales.

b) Tratándose de hechos tipificados como delito menos grave, en su ejecución se haya empleado violencia o intimidación en las personas o se haya generado grave riesgo para la vida o la integridad física de las mismas.

c) Los hechos tipificados como delito se cometan en grupo o el menor perteneciere o actuare al servicio de una banda, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

3. La duración de las medidas no podrá exceder de dos años, computándose, en su caso, a estos efectos el tiempo ya cumplido por el menor en medida cautelar, conforme a lo dispuesto en el artículo 28.5 de la presente Ley. La medida de prestaciones en beneficio de la comunidad no podrá superar las cien horas. La medida de permanencia de fin de semana no podrá superar los ocho fines de semana.

4. Las acciones u omisiones imprudentes no podrán ser sancionadas con medidas de internamiento en régimen cerrado.

5. Cuando en la postulación del Ministerio Fiscal o en la resolución dictada en el procedimiento se aprecien algunas de las circunstancias a las que se refiere el artículo 5.2 de esta Ley, sólo podrán aplicarse las medidas terapéuticas descritas en el artículo 7.1, letras d) y e) de la misma.

Artículo 10. *Reglas especiales de aplicación y duración de las medidas.*

1. Cuando se trate de los hechos previstos en el apartado 2 del artículo anterior, el Juez, oído el Ministerio Fiscal, las partes personadas y el equipo técnico, actuará conforme a las reglas siguientes:

a) si al tiempo de cometer los hechos el menor tuviere catorce o quince años de edad, la medida podrá alcanzar tres años de duración. Si se trata de prestaciones en beneficio de la comunidad, dicho máximo será de ciento cincuenta horas, y de doce fines de semana si la medida impuesta fuere la de permanencia de fin de semana.

b) si al tiempo de cometer los hechos el menor tuviere dieciséis o diecisiete años de edad, la duración máxima de la medida será de seis años; o, en sus respectivos casos, de doscientas horas de prestaciones en beneficio de la comunidad o permanencia de dieciséis fines de semana. En este supuesto, cuando el hecho revista extrema gravedad, el Juez deberá imponer una medida de internamiento en régimen cerrado de uno a seis años, complementada sucesivamente con otra medida de libertad vigilada con asistencia educativa hasta un máximo de cinco años. Sólo podrá hacerse uso de lo dispuesto en los artículos 13 y 51.1 de esta Ley Orgánica una vez transcurrido el primer año de cumplimiento efectivo de la medida de internamiento. A los efectos previstos en el párrafo anterior, se entenderán siempre supuestos de extrema gravedad aquellos en los que se apreciara reincidencia.

2. Cuando el hecho sea constitutivo de alguno de los delitos tipificados en los artículos 138, 139, 179, 180 y 571 a 580 del Código Penal, o de cualquier otro delito que tenga señalada en dicho Código o en las leyes penales especiales pena de prisión igual o superior a quince años, el Juez deberá imponer las medidas siguientes:

a) si al tiempo de cometer los hechos el menor tuviere catorce o quince años de edad, una medida de internamiento en régimen cerrado de uno a cinco años de duración, complementada en su caso por otra medida de libertad vigilada de hasta tres años.

b) si al tiempo de cometer los hechos el menor tuviere dieciséis o diecisiete años de edad, una medida de internamiento en régimen cerrado de uno a ocho años de duración, complementada en su caso por otra de libertad vigilada con asistencia educativa de hasta cinco años. En este supuesto sólo podrá hacerse uso de las facultades de modificación, suspensión o sustitución de la medida impuesta a las que se refieren los artículos 13, 40 y 51.1 de esta Ley Orgánica, cuando haya transcurrido al menos, la mitad de la duración de la medida de internamiento impuesta.

3. En el caso de que el delito cometido sea alguno de los comprendidos en los artículos 571 a 580 del Código Penal, el Juez, sin perjuicio de las demás medidas que correspondan con arreglo a esta Ley, también impondrá al menor una medida de inhabilitación absoluta por

un tiempo superior entre cuatro y quince años al de la duración de la medida de internamiento en régimen cerrado impuesta, atendiendo proporcionalmente a la gravedad del delito, el número de los cometidos y a las circunstancias que concurran en el menor.

4. Las medidas de libertad vigilada previstas en este artículo deberán ser ratificadas mediante auto motivado, previa audiencia del Ministerio Fiscal, del letrado del menor y del representante de la entidad pública de protección o reforma de menores al finalizar el internamiento, y se llevará a cabo por las instituciones públicas encargadas del cumplimiento de las penas.

Artículo 11. *Pluralidad de infracciones.*

1. Los límites máximos establecidos en el artículo 9 y en el apartado 1 del artículo 10 serán aplicables, con arreglo a los criterios establecidos en el artículo 7, apartados 3 y 4, aunque el menor fuere responsable de dos o más infracciones, en el caso de que éstas sean conexas o se trate de una infracción continuada, así como cuando un sólo hecho constituya dos o más infracciones. No obstante, en estos casos, el Juez, para determinar la medida o medidas a imponer, así como su duración, deberá tener en cuenta, además del interés del menor, la naturaleza y el número de las infracciones, tomando como referencia la más grave de todas ellas. Si pese a lo dispuesto en el artículo 20.1 de esta Ley dichas infracciones hubiesen sido objeto de diferentes procedimientos, el último Juez sentenciador señalará la medida o medidas que debe cumplir el menor por el conjunto de los hechos, dentro de los límites y con arreglo a los criterios expresados en el párrafo anterior.

2. Cuando alguno o algunos de los hechos a los que se refiere el apartado anterior fueren de los mencionados en el artículo 10.2 de esta Ley, la medida de internamiento en régimen cerrado podrá alcanzar una duración máxima de diez años para los mayores de dieciséis años y de seis años para los menores de esa edad, sin perjuicio de la medida de libertad vigilada que, de forma complementaria, corresponda imponer con arreglo a dicho artículo.

3. Cuando el menor hubiere cometido dos o más infracciones no comprendidas en el apartado 1 de este artículo será de aplicación lo dispuesto en el artículo 47 de la presente Ley.

Artículo 12. *Procedimiento de aplicación de medidas en supuestos de pluralidad de infracciones.*

1. A los fines previstos en el artículo anterior, en cuanto el Juez sentenciador tenga conocimiento de la existencia de otras medidas firmes en ejecución, pendientes de ejecución o suspendidas condicionalmente, impuestas al mismo menor por otros jueces de menores en anteriores sentencias, y una vez que la medida o medidas por él impuestas sean firmes, ordenará al secretario judicial que dé traslado del testimonio de su sentencia, por el medio más rápido posible, al Juez que haya dictado la primera sentencia firme, el cual será el competente para la ejecución de todas, asumiendo las funciones previstas en el apartado 2 de este artículo.

2. El Juez competente para la ejecución procederá a la refundición y a ordenar la ejecución de todas las medidas impuestas conforme establece el artículo 47 de esta Ley. Desde ese momento, pasará a ser competente a todos los efectos con exclusión de los órganos judiciales que hubieran dictado las posteriores resoluciones.

Artículo 13. *Modificación de la medida impuesta.*

1. El Juez competente para la ejecución, de oficio o a instancia del Ministerio Fiscal o del letrado del menor, previa audiencia de éstos e informe del equipo técnico y, en su caso, de la entidad pública de protección o reforma de menores, podrá en cualquier momento dejar sin efecto la medida impuesta, reducir su duración o sustituirla por otra, siempre que la modificación redunde en el interés del menor y se exprese suficientemente a éste el reproche merecido por su conducta.

2. En los casos anteriores, el Juez resolverá por auto motivado, contra el cual se podrán interponer los recursos previstos en la presente Ley.

Artículo 14. *Mayoría de edad del condenado.*

1. Cuando el menor a quien se le hubiere impuesto una medida de las establecidas en esta Ley alcanzase la mayoría de edad, continuará el cumplimiento de la medida hasta alcanzar los objetivos propuestos en la sentencia en que se le impuso conforme a los criterios expresados en los artículos anteriores.

2. Cuando se trate de la medida de internamiento en régimen cerrado y el menor alcance la edad de dieciocho años sin haber finalizado su cumplimiento, el Juez de Menores, oído el Ministerio Fiscal, el letrado del menor, el equipo técnico y la entidad pública de protección o reforma de menores, podrá ordenar en auto motivado que su cumplimiento se lleve a cabo en un centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria si la conducta de la persona internada no responde a los objetivos propuestos en la sentencia.

3. No obstante lo señalado en los apartados anteriores, cuando las medidas de internamiento en régimen cerrado sean impuestas a quien haya cumplido veintiún años de edad o, habiendo sido impuestas con anterioridad, no hayan finalizado su cumplimiento al alcanzar la persona dicha edad, el Juez de Menores, oídos el Ministerio Fiscal, el letrado del menor, el equipo técnico y la entidad pública de protección o reforma de menores, ordenará su cumplimiento en centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria, salvo que, excepcionalmente, entienda en consideración a las circunstancias concurrentes que procede la utilización de las medidas previstas en los artículos 13 y 51 de la presente Ley o su permanencia en el centro en cumplimiento de tal medida cuando el menor responda a los objetivos propuestos en la sentencia.

4. Cuando el menor pase a cumplir la medida de internamiento en un centro penitenciario, quedarán sin efecto el resto de medidas impuestas por el Juez de Menores que estuvieren pendientes de cumplimiento sucesivo o que estuviera cumpliendo simultáneamente con la de internamiento, si éstas no fueren compatible con el régimen penitenciario, todo ello sin perjuicio de que excepcionalmente proceda la aplicación de los artículos 13 y 51 de esta Ley.

5. La medida de internamiento en régimen cerrado que imponga el Juez de Menores con arreglo a la presente Ley se cumplirá en un centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria siempre que, con anterioridad al inicio de la ejecución de dicha medida, el responsable hubiera cumplido ya, total o parcialmente, bien una pena de prisión impuesta con arreglo al Código Penal, o bien una medida de internamiento ejecutada en un centro penitenciario conforme a los apartados 2 y 3 de este artículo.

Artículo 15. *De la prescripción.*

1. Los hechos delictivos cometidos por los menores prescriben:

1.º Con arreglo a las normas contenidas en el Código Penal, cuando se trate de los hechos delictivos tipificados en los artículos 138, 139, 179, 180 y 571 a 580 del Código Penal o cualquier otro sancionado en el Código Penal o en las leyes penales especiales con pena de prisión igual o superior a quince años.

2.º A los cinco años, cuando se trate de un delito grave sancionado en el Código Penal con pena superior a diez años.

3.º A los tres años, cuando se trate de cualquier otro delito grave.

4.º Al año, cuando se trate de un delito menos grave. 5.º A los tres meses, cuando se trate de una falta.

2. Las medidas que tengan una duración superior a los dos años prescribirán a los tres años. Las restantes medidas prescribirán a los dos años, excepto la amonestación, las prestaciones en beneficio de la comunidad y la permanencia de fin de semana, que prescribirán al año.

[. . .]

§ 40

Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial]

Ministerio de Gracia y Justicia
«BOE» núm. 260, de 17 de septiembre de 1882
Última modificación: 6 de octubre de 2015
Referencia: BOE-A-1882-6036

[. . .]

LIBRO II

Del sumario

TÍTULO I

De la denuncia

Artículo 259.

El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas.

Artículo 260.

La obligación establecida en el artículo anterior no comprende a los impúberes ni a los que no gozaren del pleno uso de su razón.

Artículo 261.

Tampoco estarán obligados a denunciar:

1.º El cónyuge del delincuente no separado legalmente o de hecho o la persona que conviva con él en análoga relación de afectividad.

2.º Los ascendientes y descendientes del delincuente y sus parientes colaterales hasta el segundo grado inclusive.

Artículo 262.

Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal

competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante.

Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.

Si la omisión en dar parte fuere de un Profesor en Medicina, Cirugía o Farmacia y tuviese relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas ni superior a 250.

Si el que hubiese incurrido en la omisión fuere empleado público, se pondrá además en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo.

Lo dispuesto en este artículo se entiende cuando la omisión no produjere responsabilidad con arreglo a las Leyes.

Artículo 263.

La obligación impuesta en el párrafo primero del art. anterior no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes. Tampoco comprenderá a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio.

Artículo 263 bis.

1. El Juez de Instrucción competente y el Ministerio Fiscal, así como los Jefes de las Unidades Orgánicas de Policía Judicial, centrales o de ámbito provincial, y sus mandos superiores podrán autorizar la circulación o entrega vigilada de drogas tóxicas, estupefacientes o sustancias psicotrópicas, así como de otras sustancias prohibidas. Esta medida deberá acordarse por resolución fundada, en la que se determine explícitamente, en cuanto sea posible, el objeto de autorización o entrega vigilada, así como el tipo y cantidad de la sustancia de que se trate. Para adoptar estas medidas se tendrá en cuenta su necesidad a los fines de investigación en relación con la importancia del delito y con las posibilidades de vigilancia. El Juez que dicte la resolución dará traslado de copia de la misma al Juzgado Decano de su jurisdicción, el cual tendrá custodiado un registro de dichas resoluciones.

También podrá ser autorizada la circulación o entrega vigilada de los equipos, materiales y sustancias a los que se refiere el artículo 371 del Código Penal, de los bienes y ganancias a que se hace referencia en el artículo 301 de dicho Código en todos los supuestos previstos en el mismo, así como de los bienes, materiales, objetos y especies animales y vegetales a los que se refieren los artículos 332, 334, 386, 399 bis, 566, 568 y 569, también del Código Penal.

2. Se entenderá por circulación o entrega vigilada la técnica consistente en permitir que remesas ilícitas o sospechosas de drogas tóxicas, sustancias psicotrópicas u otras sustancias prohibidas, los equipos, materiales y sustancias a que se refiere el apartado anterior, las sustancias por las que se haya sustituido las anteriormente mencionadas, así como los bienes y ganancias procedentes de las actividades delictivas tipificadas en los artículos 301 a 304 y 368 a 373 del Código Penal, circulen por territorio español o salgan o entren en él sin interferencia obstativa de la autoridad o sus agentes y bajo su vigilancia, con el fin de descubrir o identificar a las personas involucradas en la comisión de algún delito relativo a dichas drogas, sustancias, equipos, materiales, bienes y ganancias, así como también prestar auxilio a autoridades extranjeras en esos mismos fines.

3. El recurso a la entrega vigilada se hará caso por caso y, en el plano internacional, se adecuará a lo dispuesto en los tratados internacionales.

Los Jefes de las Unidades Orgánicas de la Policía Judicial centrales o de ámbito provincial o sus mandos superiores darán cuenta inmediata al Ministerio Fiscal sobre las autorizaciones que hubiesen otorgado de conformidad con el apartado 1 de este artículo y, si existiese procedimiento judicial abierto, al Juez de Instrucción competente.

4. La interceptación y apertura de envíos postales sospechosos de contener estupefacientes y, en su caso, la posterior sustitución de la droga que hubiese en su interior

se llevarán a cabo respetando en todo momento las garantías judiciales establecidas en el ordenamiento jurídico, con excepción de lo previsto en el artículo 584 de la presente Ley.

Artículo 264.

El que por cualquier medio diferente de los mencionados tuviere conocimiento de la perpetración de algún delito de los que deben perseguirse de oficio, deberá denunciarlo al Ministerio Fiscal, al Tribunal competente o al Juez de instrucción o municipal, o funcionario de policía, sin que se entienda obligado por esto a probar los hechos denunciados ni a formalizar querella.

El denunciador no contraerá en ningún caso otra responsabilidad que la correspondiente a los delitos que hubiese cometido por medio de la denuncia, o con su ocasión.

Artículo 265.

Las denuncias podrán hacerse por escrito o de palabra, personalmente o por medio de mandatario con poder especial.

Artículo 266.

La denuncia que se hiciere por escrito deberá estar firmada por el denunciador; y si no pudiere hacerlo, por otra persona a su ruego. La autoridad o funcionario que la recibiere rubricará y sellará todas las hojas a presencia del que la presentare, quien podrá también rubricarla por sí o por medio de otra persona a su ruego.

Artículo 267.

Cuando la denuncia sea verbal, se extenderá un acta por la autoridad o funcionario que la recibiere, en la que, en forma de declaración, se expresarán cuantas noticias tenga el denunciante relativas al hecho denunciado y a sus circunstancias, firmándola ambos a continuación. Si el denunciante no pudiere firmar, lo hará otra persona a su ruego.

Artículo 268.

El Juez, Tribunal, autoridad o funcionario que recibieren una denuncia verbal o escrita harán constar por la cédula personal o por otros medios que reputen suficientes, la identidad de la persona del denunciador.

Si éste lo exigiere, le darán un resguardo de haber formalizado la denuncia.

Artículo 269.

Formalizada que sea la denuncia, se procederá o mandará proceder inmediatamente por el Juez o funcionario a quien se hiciese a la comprobación del hecho denunciado, salvo que éste no revistiere carácter de delito, o que la denuncia fuere manifiestamente falsa. En cualquiera de estos dos casos, el Tribunal o funcionario se abstendrán de todo procedimiento, sin perjuicio de la responsabilidad en que incurran si desestimasen aquélla indebidamente.

TÍTULO II

De la querella

Artículo 270.

Todos los ciudadanos españoles, hayan sido o no ofendidos por el delito, pueden querellarse, ejercitando la acción popular establecida en el artículo 101 de esta Ley.

También pueden querellarse los extranjeros por los delitos cometidos contra sus personas o bienes o las personas o bienes de sus representados, previo cumplimiento de lo dispuesto en el artículo 280, si no estuvieren comprendidos en el último párrafo del 281.

Artículo 271.

Los funcionarios del Ministerio fiscal ejercitarán también, en forma de querella, las acciones penales en los casos en que estuvieren obligados con arreglo a lo dispuesto en el artículo 105.

Artículo 272.

La querella se interpondrá ante el Juez de instrucción competente.

Si el querellado estuviere sometido por disposición especial de la Ley a determinado Tribunal, ante éste se interpondrá la querella.

Lo mismo se hará cuando fueren varios los querellados por un mismo delito o por dos o más conexos y alguno de aquéllos estuviere sometido excepcionalmente a un Tribunal que no fuere el llamado a conocer, por regla general, del delito.

Artículo 273.

En los casos del artículo anterior, cuando se trate de un delito in fraganti o de los que no dejan señales permanentes de su perpetración, o en que fuere de temer fundadamente la ocultación o fuga del presunto culpable, el particular que intentare querellarse del delito podrá acudir desde luego al Juez de instrucción o municipal que estuviere más próximo o a cualquier funcionario de policía, a fin de que se practiquen las primeras diligencias necesarias para hacer constar la verdad de los hechos y para detener al delincuente.

Artículo 274.

El particular querellante, cualquiera que sea su fuero, quedará sometido, para todos los efectos del juicio por él promovido, al Juez de instrucción o Tribunal competente para conocer del delito objeto de la querella.

Pero podrá apartarse de la querella en cualquier tiempo, quedando, sin embargo, sujeto a las responsabilidades que pudieran resultarle por sus actos anteriores.

Artículo 275.

Si la querella fuese por delito que no pueda ser perseguido sino a instancia de parte, se entenderá abandonada por el que la hubiere interpuesto cuando dejare de instar el procedimiento dentro de los diez días siguientes a la notificación del auto en que el Juez o el Tribunal así lo hubiese acordado.

Al efecto, a los diez días de haberse practicado las últimas diligencias pedidas por el querellante, o de estar paralizada la causa por falta de instancia del mismo, mandará de oficio el Juez o Tribunal que conociere de los autos que aquél pida lo que convenga a su derecho en el término fijado en el párrafo anterior.

Artículo 276.

Se tendrá también por abandonada la querella cuando, por muerte o por haberse incapacitado el querellante para continuar la acción, no compareciere ninguno de sus herederos o representantes legales a sostenerla dentro de los treinta días siguientes a la citación que al efecto se les hará dándoles conocimiento de la querella.

Artículo 277.

La querella se presentará siempre por medio de Procurador con poder bastante y suscrita por Letrado.

Se extenderá en papel de oficio, y en ella se expresará:

1.º El Juez o Tribunal ante quien se presente.

2.º El nombre, apellidos y vecindad del querellante.

3.º El nombre, apellidos y vecindad del querellado.

En el caso de ignorarse estas circunstancias, se deberá hacer la designación del querellado por las señas que mejor pudieran darle a conocer.

4.º La relación circunstanciada del hecho, con expresión del lugar, año, mes, día y hora en que se ejecutó, si se supieren.

5.º Expresión de las diligencias que se deberán practicar para la comprobación del hecho.

6.º La petición de que se admita la querella, se practiquen las diligencias indicadas en el número anterior, se proceda a la detención y prisión del presunto culpable o a exigirle la fianza de libertad provisional, y se acuerde el embargo de sus bienes en la cantidad necesaria en los casos en que así proceda.

7.º La firma del querellante o la de otra persona a su ruego si no supiere o no pudiere firmar cuando el Procurador no tuviese poder especial para formular la querella.

Artículo 278.

Si la querella tuviere por objeto algún delito de los que solamente pueden perseguirse a instancia de parte, excepto el de violación o rapto, acompañará también la certificación que acredite haberse celebrado o intentado el acto de conciliación entre querellante y querellado.

Podrán, sin embargo, practicarse sin este requisito las diligencias de carácter urgente para la comprobación de los hechos o para la detención del delincuente, suspendiendo después el curso de los autos hasta que se acredite el cumplimiento de lo dispuesto en el párrafo anterior.

Artículo 279.

En los delitos de calumnia o injuria causadas en juicio se presentará además la licencia del Juez o Tribunal que hubiese conocido de aquél, con arreglo a lo dispuesto en el Código Penal.

Artículo 280.

El particular querellante prestará fianza de la clase y en la cuantía que fijare el Juez o Tribunal para responder de las resultas del juicio.

Artículo 281.

Quedan exentos de cumplir lo dispuesto en el artículo anterior:

1.º El ofendido y sus herederos o representantes legales.

2.º En los delitos de asesinato o de homicidio, el cónyuge del difunto o persona vinculada a él por una análoga relación de afectividad, los ascendientes y descendientes y sus parientes colaterales hasta el segundo grado inclusive, los herederos de la víctima y los padres, madres e hijos del delincuente.

3.º Las asociaciones de víctimas y las personas jurídicas a las que la ley reconoce legitimación para defender los derechos de las víctimas siempre que el ejercicio de la acción penal hubiera sido expresamente autorizado por la propia víctima.

La exención de fianza no es aplicable a los extranjeros si no les correspondiere en virtud de tratados internacionales o por el principio de reciprocidad.»

TÍTULO III

De la Policía judicial

Artículo 282.

La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las

circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal.

Si el delito fuera de los que sólo pueden perseguirse a instancia de parte legítima, tendrán la misma obligación expresada en el párrafo anterior, si se les requiere al efecto. La ausencia de denuncia no impedirá la práctica de las primeras diligencias de prevención y aseguramiento de los delitos relativos a la propiedad intelectual e industrial.

Artículo 282 bis.

1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.

Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.

4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.

6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.

Artículo 283.

Constituirán la Policía judicial y serán auxiliares de los Jueces y Tribunales competentes en materia penal y del Ministerio fiscal, quedando obligados a seguir las instrucciones que de aquellas autoridades reciban a efectos de la investigación de los delitos y persecución de los delincuentes:

Primero. Las Autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales.

Segundo. Los empleados o subalternos de la policía de seguridad, cualquiera que sea su denominación.

Tercero. Los Alcaldes, Tenientes de Alcalde y Alcaldes de barrio.

Cuarto. Los Jefes, Oficiales e individuos de la Guardia Civil o de cualquier otra fuerza destinada a la persecución de malhechores.

Quinto. Los Serenos, Celadores y cualesquiera otros Agentes municipales de policía urbana o rural.

Sexto. Los Guardas de montes, campos y sembrados, jurados o confirmados por la Administración.

Séptimo. Los funcionarios del Cuerpo especial de Prisiones.

Octavo. Los Agentes judiciales y los subalternos de los Tribunales y Juzgados.

Noveno. El personal dependiente de la Jefatura Central de Tráfico, encargado de la investigación técnica de los accidentes.

Artículo 284.

1. Inmediatamente que los funcionarios de la Policía judicial tuvieren conocimiento de un delito público o fueren requeridos para prevenir la instrucción de diligencias por razón de algún delito privado, lo participarán a la autoridad judicial o al representante del Ministerio Fiscal, si pudieren hacerlo sin cesar en la práctica de las diligencias de prevención. En otro caso, lo harán así que las hubieren terminado.

2. No obstante, cuando no exista autor conocido del delito la Policía Judicial conservará el atestado a disposición del Ministerio Fiscal y de la autoridad judicial, sin enviárselo, salvo que concurra alguna de las siguientes circunstancias:

a) Que se trate de delitos contra la vida, contra la integridad física, contra la libertad e indemnidad sexuales o de delitos relacionados con la corrupción;

b) Que se practique cualquier diligencia después de transcurridas setenta y dos horas desde la apertura del atestado y éstas hayan tenido algún resultado; o

c) Que el Ministerio Fiscal o la autoridad judicial soliciten la remisión.

De conformidad con el derecho reconocido en el artículo 6 de la Ley 4/2015, de 27 de abril, del Estatuto de la Víctima del delito, la Policía Judicial comunicará al denunciante que en caso de no ser identificado el autor en el plazo de setenta y dos horas, las actuaciones no se remitirán a la autoridad judicial, sin perjuicio de su derecho a reiterar la denuncia ante la fiscalía o el juzgado de instrucción.

3. Si hubieran recogido armas, instrumentos o efectos de cualquier clase que pudieran tener relación con el delito y se hallen en el lugar en que éste se cometió o en sus inmediaciones, o en poder del reo o en otra parte conocida, extenderán diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, que incluirá una descripción minuciosa para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo, que podrá ser sustituida por un reportaje gráfico. La diligencia será firmada por la persona en cuyo poder fueren hallados.

4. La incautación de efectos que pudieran pertenecer a una víctima del delito será comunicada a la misma. La persona afectada por la incautación podrá recurrir en cualquier momento la medida ante el juez de instrucción de conformidad con lo dispuesto en el párrafo tercero del artículo 334.

Artículo 285.

Si concurriere algún funcionario de Policía judicial de categoría superior a la del que estuviese actuando, deberá éste darle conocimiento de cuanto hubiese practicado, poniéndose desde luego a su disposición.

Artículo 286.

Cuando el Juez de instrucción o el municipal se presentaren a formar el sumario, cesarán las diligencias de prevención que estuviere practicando cualquier Autoridad o agente de policía; debiendo éstos entregarlas en el acto a dicho Juez, así como los efectos relativos al delito que se hubiesen recogido, y poniendo a su disposición a los detenidos, si los hubiese.

Artículo 287.

Los funcionarios que constituyen la Policía judicial practicarán sin dilación, según sus atribuciones respectivas, las diligencias que los funcionarios del Ministerio fiscal les encomienden para la comprobación del delito y averiguación de los delincuentes y todas las demás que durante el curso de la causa les encargaren los Jueces de instrucción y municipales.

Artículo 288.

El Ministerio fiscal, los Jueces de instrucción y los municipales podrán entenderse directamente con los funcionarios de Policía judicial, cualquiera que sea su categoría, para

todos los efectos de este título; pero si el servicio que de ellos exigiesen admitiese espera, deberán acudir al superior respectivo del funcionario de Policía judicial, mientras no necesitasen del inmediato auxilio de éste.

Artículo 289.

El funcionario de Policía judicial que por cualquier causa no pueda cumplir el requerimiento o la orden que hubiese recibido del Ministerio fiscal, del Juez de instrucción, del Juez municipal, o de la Autoridad o agente que hubiese prevenido las primeras diligencias, lo pondrá inmediatamente en conocimiento del que haya hecho el requerimiento o dado la orden para que provea de otro modo a su ejecución.

Artículo 290.

Si la causa no fuere legítima, el que hubiese dado la orden o hecho el requerimiento lo pondrá en conocimiento del superior jerárquico del que se excuse para que le corrija disciplinariamente, a no ser que hubiere incurrido en mayor responsabilidad con arreglo a las leyes.

El superior jerárquico comunicará a la Autoridad o funcionario que le hubiere dado la queja la resolución que adopte respecto de su subordinado.

Artículo 291.

El jefe de cualquier fuerza pública que no pudiere prestar el auxilio que por los Jueces de instrucción o municipales o por un funcionario de Policía judicial le fuere pedido se atendrá también a lo dispuesto en el artículo 289.

El que hubiere hecho el requerimiento lo pondrá en conocimiento del Jefe superior inmediato del que se excusare en la forma y para el objeto expresado en los párrafos del artículo anterior.

Artículo 292.

Los funcionarios de Policía judicial extenderán, bien en papel sellado, bien en papel común, un atestado de las diligencias que practiquen, en el cual especificarán con la mayor exactitud los hechos por ellos averiguados, insertando las declaraciones e informes recibidos y anotando todas las circunstancias que hubiesen observado y pudiesen ser prueba o indicio del delito.

La Policía Judicial remitirá con el atestado un informe dando cuenta de las detenciones anteriores y de la existencia de requisitorias para su llamamiento y busca cuando así conste en sus bases de datos.

Artículo 293.

El atestado será firmado por el que lo haya extendido, y si usare sello lo estampará con su rúbrica en todas las hojas.

Las personas presentes, peritos y testigos que hubieren intervenido en las diligencias relacionadas en el atestado serán invitadas a firmarlo en la parte a ellos referente. Si no lo hicieren, se expresará la razón.

Artículo 294.

Si no pudiere redactar el atestado el funcionario a quien correspondiese hacerlo, se sustituirá por una relación verbal circunstanciada, que reducirá a escrito de un modo fehaciente el funcionario del Ministerio fiscal, el Juez de instrucción o el municipal a quien deba presentarse el atestado, manifestándose el motivo de no haberse redactado en la forma ordinaria.

Artículo 295.

En ningún caso los funcionarios de Policía Judicial podrán dejar transcurrir más de veinticuatro horas sin dar conocimiento a la autoridad judicial o al Ministerio Fiscal de las

diligencias que hubieran practicado, salvo en los supuestos de fuerza mayor y en el previsto en el apartado 2 del artículo 284.

Los que infrinjan esta disposición serán corregidos disciplinariamente con multa de 250 a 1.000 pesetas, si la omisión no mereciere la calificación de delito, y al propio tiempo será considerada dicha infracción como falta grave la primera vez y como falta muy grave las siguientes.

Los que, sin exceder el tiempo de las veinticuatro horas, demorasen más de lo necesario el dar conocimiento, serán corregidos disciplinariamente con una multa de 100 a 350 pesetas, y además esta infracción constituirá a efectos del expediente personal del interesado, falta leve la primera vez, grave las dos siguientes y muy grave las restantes.

Artículo 296.

Cuando hubieren practicado diligencias por orden o requerimiento de la Autoridad judicial o del Ministerio fiscal, comunicarán el resultado obtenido en los plazos que en la orden o en el requerimiento se hubiesen fijado.

Artículo 297.

Los atestados que redactaren y las manifestaciones que hicieren los funcionarios de Policía judicial, a consecuencia de las averiguaciones que hubiesen practicado, se considerarán denuncias para los efectos legales.

Las demás declaraciones que prestaren deberán ser firmadas, y tendrán el valor de declaraciones testificales en cuanto se refieran a hechos de conocimiento propio.

En todo caso, los funcionarios de Policía judicial están obligados a observar estrictamente las formalidades legales en cuantas diligencias practiquen, y se abstendrán bajo su responsabilidad de usar medios de averiguación que la Ley no autorice.

Artículo 298.

Los Jueces de instrucción y los Fiscales calificarán en un registro reservado el comportamiento de los funcionarios que bajo su inspección prestan servicios de Policía judicial; y cada semestre, con referencia a dicho registro, comunicarán a los superiores de cada uno de aquéllos, para los efectos a que hubiere lugar, la calificación razonada de su comportamiento.

Cuando los funcionarios de Policía judicial que hubieren de ser corregidos disciplinariamente con arreglo a esta Ley fuesen de categoría superior a la de la Autoridad judicial o fiscal que entendiesen en las diligencias en que se hubiere cometido la falta, se abstendrán éstos de imponer por sí mismos la corrección, limitándose a poner lo ocurrido en conocimiento del jefe inmediato del que debiere ser corregido.

[. . .]

TÍTULO V

De la comprobación del delito y averiguación del delincuente

[. . .]

CAPÍTULO II

Del cuerpo del delito

Artículo 334.

El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida.

El Secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.

La diligencia será firmada por la persona en cuyo poder fueren hallados, notificándose a la misma el auto en que se mande recogerlos.

La persona afectada por la incautación podrá recurrir en cualquier momento la medida ante el Juez de Instrucción. Este recurso no requerirá de la intervención de abogado cuando sea presentado por terceras personas diferentes del imputado. El recurso se entenderá interpuesto cuando la persona afectada por la medida o un familiar suyo mayor de edad hubieran expresado su disconformidad en el momento de la misma.

Los efectos que pertenecieran a la víctima del delito serán restituidos inmediatamente a la misma, salvo que excepcionalmente debieran ser conservados como medio de prueba o para la práctica de otras diligencias, y sin perjuicio de su restitución tan pronto resulte posible. Los efectos serán también restituidos inmediatamente cuando deban ser conservados como medio de prueba o para la práctica de otras diligencias, pero su conservación pueda garantizarse imponiendo al propietario el deber de mantenerlos a disposición del Juez o Tribunal. La víctima podrá, en todo caso, recurrir esta decisión conforme a lo dispuesto en el párrafo anterior.

Artículo 335.

Siendo habida la persona o cosa objeto del delito, el Juez instructor describirá detalladamente su estado y circunstancias, y especialmente todas las que tuviesen relación con el hecho punible.

Si por tratarse de delito de falsificación cometida en documentos o efectos existentes en dependencias de las Administraciones Públicas hubiere imprescindible necesidad de tenerlos a la vista para su reconocimiento pericial y examen por parte del Juez o Tribunal, el Secretario judicial los reclamará a las correspondientes Autoridades, sin perjuicio de devolverlos a los respectivos Centros oficiales después de terminada la causa.

Artículo 336.

En los casos de los dos artículos anteriores ordenará también el Juez el reconocimiento por peritos, siempre que esté indicado para apreciar mejor la relación con el delito, de los lugares, armas, instrumentos y efectos a que dichos artículos se refieren, haciéndose constar por diligencia el reconocimiento y el informe pericial.

A esta diligencia podrán asistir también el procesado y su defensor en los términos expresados en el artículo 333.

Artículo 337.

Cuando en el acto de describir la persona o cosa objeto del delito y los lugares, armas, instrumentos o efectos relacionados con el mismo, estuvieren presentes o fueren conocidas personas que puedan declarar acerca del modo y forma con que aquél hubiese sido cometido, y de las causas de las alteraciones que se observaren en dichos lugares, armas, instrumentos o efectos, acerca de su estado anterior, serán examinadas inmediatamente después de la descripción, y sus declaraciones se considerarán como complemento de ésta.

Artículo 338.

Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito.

Artículo 339.

Si fuere conveniente recibir algún informe pericial sobre los medios empleados para la desaparición del cuerpo del delito, o sobre las pruebas de cualquiera clase que en su defecto

se hubiesen recogido, el Juez lo ordenará inmediatamente del modo prevenido en el capítulo VII de este mismo título.

[. . .]

Artículo 364.

En los delitos de robo, hurto, estafa y en cualquiera otro en que deba hacerse constar la preexistencia de las cosas robadas, hurtadas o estafadas, si no hubiere testigos presenciales del hecho, se recibirá información sobre los antecedentes del que se presentare como agraviado, y sobre todas las circunstancias que ofrecieren indicios de hallarse éste poseyendo aquéllas al tiempo en que resulte cometido el delito.

Artículo 365.

Cuando para la calificación del delito o de sus circunstancias fuere necesario estimar el valor de la cosa que hubiere sido su objeto o el importe del perjuicio causado o que hubiera podido causarse, el Juez oirá sobre ello al dueño o perjudicado, y acordará después el reconocimiento pericial en la forma determinada en el capítulo VII de este mismo título. El Secretario judicial facilitará a los peritos nombrados las cosas y elementos directos de apreciación sobre que hubiere de recaer el informe. Si tales efectos no estuvieren a disposición del órgano judicial, el Secretario judicial les suministrará los datos oportunos que se pudieren reunir, a fin de que, en tal caso, hagan la tasación y regulación de perjuicios de un modo prudente, con arreglo a los datos suministrados.

La valoración de las mercancías sustraídas en establecimientos comerciales se fijará atendiendo a su precio de venta al público.

Artículo 366.

Las diligencias prevenidas en este capítulo y en el anterior se practicarán con preferencia a las demás del sumario, no suspendiéndose su ejecución sino para asegurar la persona del presunto culpable o para dar el auxilio necesario a los agraviados por el delito.

Artículo 367.

En ningún caso admitirá el Juez durante el sumario reclamaciones ni tercerías que tengan por objeto la devolución de los efectos que constituyen el cuerpo del delito, cualquiera que sea su clase y la persona que los reclame.

CAPÍTULO II BIS

De la destrucción y la realización anticipada de los efectos judiciales

Artículo 367 bis.

Tendrán la consideración de efectos judiciales, en el orden penal, todos aquellos bienes puestos a disposición judicial, embargados, incautados o aprehendidos en el curso de un procedimiento penal.

Artículo 367 ter.

1. Podrá decretarse la destrucción de los efectos judiciales, dejando muestras suficientes, cuando resultare necesaria o conveniente por la propia naturaleza de los efectos intervenidos o por el peligro real o potencial que comporte su almacenamiento o custodia, previa audiencia al Ministerio Fiscal y al propietario, si fuere conocido, o a la persona en cuyo poder fueron hallados los efectos cuya destrucción se pretende.

Cuando se trate de drogas tóxicas, estupefacientes o sustancias psicotrópicas, la autoridad administrativa bajo cuya custodia se encuentren, una vez realizados los informes analíticos pertinentes, asegurada la conservación de las muestras mínimas e imprescindibles

que, conforme a criterios científicos, resulten necesarias para garantizar ulteriores comprobaciones o investigaciones, y previa comunicación al Juez instructor, procederá a su inmediata destrucción si, trascurrido el plazo de un mes desde que se efectuó aquella, la autoridad judicial no hubiera ordenado mediante resolución motivada la conservación íntegra de dichas sustancias. En todo caso, lo conservado se custodiará siempre a disposición del órgano judicial competente.

2. En todo caso, el Secretario judicial extenderá la oportuna diligencia y, si se hubiera acordado la destrucción, deberá quedar constancia en los autos de la naturaleza, calidad, cantidad, peso y medida de los efectos destruidos. Si no hubiese tasación anterior, también se dejará constancia de su valor cuando su fijación fuere imposible después de la destrucción.

3. Lo dispuesto en los dos apartados anteriores será también aplicable a los efectos intervenidos en relación con la comisión de delitos contra la propiedad intelectual e industrial. Podrá igualmente procederse a su destrucción anticipada una vez que tales efectos hayan sido examinados pericialmente, asegurando la conservación de las muestras que resulten necesarias para garantizar ulteriores comprobaciones o investigaciones, salvo que la autoridad judicial acuerde mediante resolución motivada su conservación íntegra en el plazo de un mes desde la solicitud de destrucción.

4. Si los objetos no pudieren, por su naturaleza, conservarse en su forma primitiva, el Juez resolverá lo que estime conveniente para conservarlos del mejor modo posible.

Artículo 367 quáter.

1. Podrán realizarse los efectos judiciales de lícito comercio, sin esperar al pronunciamiento o firmeza del fallo, y siempre que no se trate de piezas de convicción o que deban quedar a expensas del procedimiento, en cualquiera de los casos siguientes:

a) Cuando sean perecederos.

b) Cuando su propietario haga expreso abandono de ellos.

c) Cuando los gastos de conservación y depósito sean superiores al valor del objeto en sí.

d) Cuando su conservación pueda resultar peligrosa para la salud o seguridad pública, o pueda dar lugar a una disminución importante de su valor, o pueda afectar gravemente a su uso y funcionamiento habituales.

e) Cuando se trate de efectos que, sin sufrir deterioro material, se deprecien sustancialmente por el transcurso del tiempo.

f) Cuando, debidamente requerido el propietario sobre el destino del efecto judicial, no haga manifestación alguna.

2. Cuando concurra alguno de los supuestos previstos en el apartado anterior, el juez, de oficio o a instancia del Ministerio Fiscal, de las partes o de la Oficina de Recuperación y Gestión de Activos, y previa audiencia del interesado, acordará la realización de los efectos judiciales, salvo que concurra alguna de las siguientes circunstancias:

a) Esté pendiente de resolución el recurso interpuesto por el interesado contra el embargo o decomiso de los bienes o efectos.

b) La medida pueda resultar desproporcionada, a la vista de los efectos que pudiera suponer para el interesado y, especialmente, de la mayor o menor relevancia de los indicios en que se hubiera fundado la resolución cautelar de decomiso.

3. No obstante lo dispuesto en los apartados anteriores, cuando el bien de que se trate esté embargado en ejecución de un acuerdo adoptado por una autoridad judicial extranjera en aplicación de la Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea, su realización no podrá llevarse a cabo sin obtener previamente la autorización de la autoridad judicial extranjera.

Artículo 367 quinquies.

1. La realización de los efectos judiciales podrá consistir en:

a) La entrega a entidades sin ánimo de lucro o a las Administraciones públicas.

b) La realización por medio de persona o entidad especializada.
c) La subasta pública.

2. Podrá entregarse el efecto judicial a entidades sin ánimo de lucro o a las Administraciones públicas cuando sea de ínfimo valor o se prevea que la realización por medio de persona o entidad especializada o por medio de subasta pública será antieconómica.

3. La realización de los efectos judiciales se llevará a cabo conforme al procedimiento que se determine reglamentariamente. No obstante lo anterior, previamente a acordarla se concederá audiencia al Ministerio Fiscal y a los interesados.

El producto de la realización de los efectos, bienes, instrumentos y ganancias se aplicará a los gastos que se hubieran causado en la conservación de los bienes y en el procedimiento de realización de los mismos, y la parte sobrante se ingresará en la cuenta de consignaciones del juzgado o tribunal, quedando afecta al pago de las responsabilidades civiles y costas que se declaren, en su caso, en el procedimiento. También podrá asignarse total o parcialmente de manera definitiva, en los términos y por el procedimiento que reglamentariamente se establezcan, a la Oficina de Recuperación y Gestión de Activos y a los órganos del Ministerio Fiscal encargados de la represión de las actividades de las organizaciones criminales. Todo ello sin perjuicio de lo dispuesto para el Fondo de bienes decomisados por tráfico ilícito de drogas y otros delitos relacionados.

En el caso de realización de un bien embargado o decomisado por orden de una autoridad judicial extranjera se aplicará lo dispuesto en la Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea.

Artículo 367 sexies.

1. Podrá autorizarse la utilización provisional de los bienes o efectos decomisados cautelarmente en los siguientes casos:

a) Cuando concurran las circunstancias expresadas en las letras b) a f) del apartado 1 del artículo 367 quater, y la utilización de los efectos permita a la Administración un aprovechamiento de su valor mayor que con la realización anticipada, o no se considere procedente la realización anticipada de los mismos.
b) Cuando se trate de efectos especialmente idóneos para la prestación de un servicio público.

2. Cuando concurra alguno de los supuestos previstos en el apartado anterior, el juez, de oficio o a instancia del Ministerio Fiscal o de la Oficina de Recuperación y Gestión de activos, y previa audiencia del interesado, autorizará la utilización provisional de los efectos judiciales, salvo que concurra alguna de las circunstancias expresadas en el párrafo segundo del apartado 2 del artículo 367 quater.

3. Corresponderá a la Oficina de Recuperación y Gestión de activos resolver, conforme a lo previsto legal y reglamentariamente, sobre la adjudicación del uso de los efectos decomisados cautelarmente y sobre las medidas de conservación que deban ser adoptadas. La oficina informará al juez o tribunal, y al Fiscal, de lo que hubiera acordado.

Artículo 367 septies.

El juez o tribunal, de oficio o a instancia del Ministerio Fiscal o de la propia Oficina de Recuperación y Gestión de activos, podrá encomendar la localización, la conservación y la administración de los efectos, bienes, instrumentos y ganancias procedentes de actividades delictivas cometidas en el marco de una organización criminal a la Oficina de Recuperación y Gestión de Activos.

La organización y funcionamiento de dicha Oficina se regularán reglamentariamente.

CAPÍTULO III

De la identidad del delincuente y de sus circunstancias personales

Artículo 368.

Cuantos dirijan cargo a determinada persona deberán reconocerla judicialmente, si el Juez instructor, los acusadores o el mismo inculpado conceptúan fundamentalmente precisa la diligencia para la identificación de este último, con relación a los designantes, a fin de que no ofrezca duda quién es la persona a que aquellos se refieren.

Artículo 369.

La diligencia de reconocimiento se practicará poniendo a la vista del que hubiere de verificarlo la persona que haya de ser reconocida, haciéndola comparecer en unión con otras de circunstancias exteriores semejantes. A presencia de todas ellas, o desde un punto en que no pudiere ser visto, según al Juez pareciere más conveniente, el que deba practicar el reconocimiento manifestará si se encuentra en la rueda o grupo la persona a quien hubiese hecho referencia en sus declaraciones, designándola, en caso afirmativo, clara y determinadamente.

En la diligencia que se extienda se harán constar todas las circunstancias del acto, así como los nombres de todos los que hubiesen formado la rueda o grupo.

Artículo 370.

Cuando fueren varios los que hubieren de reconocer a una persona, la diligencia expresada en el artículo anterior deberá practicarse separadamente con cada uno de ellos, sin que puedan comunicarse entre sí hasta que se haya efectuado el último reconocimiento.

Cuando fueren varios los que hubieren de ser reconocidos por una misma persona, podrá hacerse el reconocimiento de todos en un solo acto.

Artículo 371.

El que detuviere o prendiere a algún presunto culpable tomará las precauciones necesarias para que el detenido o preso no haga en su persona o traje alteración alguna que pueda dificultar su reconocimiento por quien corresponda.

Artículo 372.

Análogas precauciones deberán tomar los Alcaides de las cárceles y los Jefes de lo depósitos de detenidos; y si en los establecimientos de su cargo hubiere traje reglamentario, conservarán cuidadosamente el que lleven los presos o detenidos al ingresar en el establecimiento, a fin de que puedan vestirlo cuantas veces fuere conveniente para diligencias de reconocimiento.

Artículo 373.

Si se originase alguna duda sobre la identidad del procesado, se procurará acreditar ésta por cuantos medios fueren conducentes al objeto.

Artículo 374.

El Juez hará constar, con la minuciosidad posible, las señas personales del procesado, a fin de que la diligencia pueda servir de prueba de su identidad.

Artículo 375.

Para acreditar la edad del procesado y comprobar la identidad de su persona, el Secretario judicial traerá al sumario certificación de su inscripción de nacimiento en el Registro civil o de su partida de bautismo, si no estuviere inscrito en el Registro.

En todo caso, cuando no fuere posible averiguar el Registro civil o parroquia en que deba constar el nacimiento o el bautismo del procesado, o no existiesen su inscripción y partida; y cuando por manifestar el procesado haber nacido en punto lejano hubiere necesidad de emplear mucho tiempo en traer a la causa la certificación oportuna, no se detendrá el sumario, y se suplirá el documento del artículo anterior por informes que acerca de la edad del procesado, y previo su examen físico, dieren los Médicos forenses o los nombrados por el Juez.

Artículo 376.

Cuando no ofreciere duda la identidad del procesado, y conocidamente tuviese la edad que el Código penal requiere para poderle exigir la responsabilidad criminal en toda su extensión, podrá prescindirse de la justificación expresada en el artículo anterior, si su práctica ofreciese alguna dificultad u ocasionase dilaciones extraordinarias.

En las actuaciones sucesivas y durante el juicio, el procesado será designado con el nombre con que fuere conocido o con el que él mismo dijere tener.

Artículo 377.

Si el Juez instructor lo considerase conveniente, podrá pedir informes sobre el procesado a las Alcaldías o a los correspondientes funcionarios de policía del pueblo o pueblos en que hubiese residido.

Estos informes serán fundados, y si no fuere posible fundarlos, se manifestará la causa que lo impidiere.

Los que los dieren no contraerán responsabilidad alguna, salvo en el caso de dolo o negligencia grave.

Artículo 378.

Podrá además el Juez recibir declaración acerca de la conducta del procesado a todas las personas que por el conocimiento que tuvieren de éste puedan ilustrarle sobre ello.

Artículo 379.

Se traerán a la causa los antecedentes penales del procesado, pidiendo los anteriores a la creación del Registro Central de Penados de 2 de octubre de 1878, a los Juzgados donde se presuma que puedan en su caso constar, y los posteriores exclusivamente al Ministerio de Gracia y Justicia.

El Jefe del Registro en el Ministerio está obligado a dar los antecedentes que se le reclamen, o certificación negativa, en su caso, en el improrrogable término de tres días, a contar desde aquel en que se reciba la petición, justificando, si así no lo hiciere, la causa legítima que lo hubiese impedido.

En los Juzgados se atenderá también preferentemente al cumplimiento de este servicio, debiendo ser corregidos disciplinariamente los funcionarios que lo posterguen.

Artículo 380.

Si el procesado fuere mayor de nueve años y menor de quince, el Juez recibirá información acerca del criterio del mismo, y especialmente de su aptitud para apreciar la criminalidad del hecho que hubiese dado motivo a la causa.

En esta información serán oídas las personas que puedan deponer con acierto por sus circunstancias personales y por las relaciones que hayan tenido con el procesado antes y después de haberse ejecutado el hecho. En su defecto se nombrarán dos Profesores de instrucción primaria para que, en unión del Médico forense o del que haga sus veces, examinen al procesado y emitan su dictamen.

Artículo 381.

Si el Juez advirtiese en el procesado indicios de enajenación mental, le someterá inmediatamente a la observación de los Médicos forenses en el establecimiento en que estuviese preso, o en otro público si fuere más a propósito o estuviese en libertad.

Los Médicos darán en tal caso su informe del modo expresado en el capítulo VII de este título.

Artículo 382.

Sin perjuicio de lo dispuesto en el artículo anterior, el Juez recibirá información acerca de la enajenación mental del procesado, en la forma prevenida en el artículo 380.

Artículo 383.

Si la demencia sobreviniera después de cometido el delito, concluso que sea el sumario se mandará archivar la causa por el Tribunal competente hasta que el procesado recobre la salud, disponiéndose además respecto de éste lo que el Código Penal prescribe para los que ejecutan el hecho en estado de demencia.

Si hubiese algún otro procesado por razón del mismo delito que no se encontrase en el caso del anterior, continuará la causa solamente en cuanto al mismo.

Artículo 384.

Desde que resultare del sumario algún indicio racional de criminalidad contra determinada persona, se dictará auto declarándola procesada y mandando que se entiendan con ella las diligencias en la forma y del modo dispuesto en este título y en los demás de esta Ley.

El procesado podrá, desde el momento de serlo, aconsejarse de Letrado, mientras no estuviere incomunicado, y valerse de él, bien para instar la pronta terminación del sumario, bien para solicitar la práctica de diligencias que le interesen, y para formular pretensiones que afecten a su situación. En el primer caso podrán recurrir en queja a la Audiencia, y en los otros dos apelar para ante la misma si el Juez instructor no accediese a sus deseos.

Estas apelaciones no serán admisibles más que en un solo efecto.

Para cumplir lo determinado en este artículo, el Juez instructor dispondrá que el procesado menor de edad sea habilitado de Procurador y Abogado, a no ser que él mismo o su representante legal designen personas que merezcan su confianza para dicha representación y defensa.

Contra los autos que dicten los Jueces de instrucción, decretando el procesamiento de alguna persona, podrá utilizarse, por la representación de ésta, recurso de reforma dentro de los tres días siguientes al de haberle sido notificada la resolución; y contra los autos denegatorios de la reforma podrá ser interpuesto recurso de apelación en un efecto dentro de los cinco días siguientes al de la notificación del auto denegatorio a la representación recurrente. También podrá ser interpuesto el recurso de apelación en un efecto subsidiariamente con el de reforma, en cuyo caso, el Juez instructor declarará admitido aquél al denegar éste. Si se diera lugar a la reforma, quedando sin efecto los procesamientos antes acordados, se estará a lo preceptuado en el párrafo siguiente, en cuanto a la reproducción de la solicitud de procesamiento ante la Audiencia.

Contra los autos denegatorios de procesamiento, sólo se concederá a quien haya solicitado éstos el recurso de reforma, utilizándolo dentro de los tres días siguientes al de la notificación. Contra los autos denegatorios de la reforma así pretendida, no se podrá utilizar recurso de apelación ni ningún otro recurso; pero podrá reproducirse ante la Audiencia correspondiente la petición de procesamiento formulada por la parte a quien le haya sido denegada, cuando, personada ante dicho Tribunal, si hace uso de tal derecho, evacue el traslado a que se refiere el artículo 627 de esta misma Ley, precisamente dentro del término por el cual le haya sido conferido dicho traslado. El Tribunal, en tales casos, al dictar el auto que ordena el artículo 630, resolverá fundadamente lo que proceda; y sin que pueda dejar al criterio del instructor la resolución, cuando estime procedentes las declaraciones de procesamiento solicitadas, mandará al Juez instructor que las haga. Los procesados a quienes estas resoluciones del instructor se refieran podrán utilizar directamente el recurso de apelación en un efecto, sin necesidad de que utilicen previamente el de reforma.

Cuando la resolución del recurso de reforma interpuesto contra un auto denegatorio de procesamiento sea favorable al recurrente y, por tanto, se acuerde el procesamiento primeramente solicitado contra la resolución en que así se declara, podrán las

representaciones de los procesados a quienes afecte utilizar los mismos recursos de reforma y apelación otorgados a los procesados directamente en este mismo artículo.

Artículo 384 bis.

Firme un auto de procesamiento y decretada la prisión provisional por delito cometido por persona integrada o relacionada con bandas armadas o individuos terroristas o rebeldes, el procesado que estuviere ostentando función o cargo público quedará automáticamente suspendido en el ejercicio del mismo mientras dure la situación de prisión.

[. . .]

CAPÍTULO VII

Del informe pericial

Artículo 456.

El Juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos.

Artículo 457.

Los peritos pueden ser o no titulares.

Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración.

Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte.

Artículo 458.

El Juez se valdrá de peritos titulares con preferencia a los que no tuviesen título.

Artículo 459.

Todo reconocimiento pericial se hará por dos peritos.

Se exceptúa el caso en que no hubiese más de uno en el lugar y no fuere posible esperar la llegada de otro sin graves inconvenientes para el curso del sumario.

Artículo 460.

El nombramiento se hará saber a los peritos por medio de oficio, que les será entregado por alguacil o portero del Juzgado, con las formalidades prevenidas para la citación de los testigos, reemplazándose la cédula original, para los efectos del artículo 175, por un atestado que extenderá el alguacil o portero encargado de la entrega.

Artículo 461.

Si la urgencia del caso lo exige, podrá hacerse el llamamiento verbalmente de orden del Juez, haciéndolo constar así en los autos; pero extendiendo siempre el atestado prevenido en el artículo anterior el encargado del cumplimiento de la orden de llamamiento.

Artículo 462.

Nadie podrá negarse a acudir al llamamiento del Juez para desempeñar un servicio pericial, si no estuviese legítimamente impedido.

En este caso deberá ponerlo en conocimiento del Juez en el acto de recibir el nombramiento, para que se provea a lo que haya lugar.

Artículo 463.

El perito que sin alegar excusa fundada deje de acudir al llamamiento del Juez o se niegue a prestar el informe, incurrirá en las responsabilidades señaladas para los testigos en el artículo 420.

Artículo 464.

No podrán prestar informe pericial acerca del delito, cualquiera que sea la persona ofendida, los que según el artículo 416 no están obligados a declarar como testigos.

El perito que, hallándose comprendido en alguno de los casos de dicho artículo, preste el informe sin poner antes esa circunstancia en conocimiento del Juez que le hubiese nombrado incurrirá en la multa de 200 a 5.000 euros, a no ser que el hecho diere lugar a responsabilidad criminal.

Artículo 465.

Los que presten informe como peritos en virtud de orden judicial tendrán derecho a reclamar los honorarios e indemnizaciones que sean justas, si no tuvieren, en concepto de tales peritos, retribución fija satisfecha por el Estado, por la Provincia o por el Municipio.

Artículo 466.

Hecho el nombramiento de peritos, el Secretario judicial lo notificará inmediatamente al Ministerio Fiscal, al actor particular, si lo hubiere, como al procesado, si estuviere a disposición del Juez o se encontrare en el mismo lugar de la instrucción, o a su representante si lo tuviere.

Artículo 467.

Si el reconocimiento e informe periciales pudieren tener lugar de nuevo en el juicio oral, los peritos nombrados no podrán ser recusados por las partes.

Si no pudiere producirse en el juicio oral, habrá lugar a la recusación.

Artículo 468.

Son causa de recusación de los peritos:

1.º El parentesco de consanguinidad o de afinidad dentro del cuarto grado con el querellante o con el reo.

2.º El interés directo o indirecto en la causa o en otra semejante.

3.º La amistad íntima o la enemistad manifiesta.

Artículo 469.

El actor o el procesado que intente recusar al perito o peritos nombrados por el Juez deberá hacerlo por escrito antes de empezar la diligencia pericial, expresando la causa de la recusación y la prueba testifical que ofrezca, y acompañando la documental o designando el lugar en que ésta se halle si no la tuviere a su disposición.

Para la presentación de este escrito no estará obligado a valerse de Procurador.

Artículo 470.

El Juez, sin levantar mano, examinará los documentos que produzca el recusante y oirá a los testigos que presente en el acto, resolviendo lo que estime justo respecto de la recusación.

Si hubiere lugar a ella, suspenderá el acto pericial por el tiempo estrictamente necesario para nombrar el perito que haya de sustituir al recusado, hacérselo saber y constituirse el nombrado en el lugar correspondiente.

Si no la admitiere, se procederá como si no se hubiese usado de la facultad de recusar.

Cuando el recusante no produjese los documentos, pero designare el archivo o lugar en que se encuentren, se reclamarán por el Secretario judicial, y el Juez instructor los

examinará una vez recibidos sin detener por esto el curso de las actuaciones; y si de ellos resultase justificada la causa de la recusación, anulará el informe pericial que se hubiese dado, mandando que se practique de nuevo esta diligencia.

Artículo 471.

En el caso del párrafo segundo del artículo 467, el querellante tendrá derecho a nombrar a su costa un perito que intervenga en el acto pericial.

El mismo derecho tendrá el procesado.

Si los querellantes o los procesados fuesen varios, se pondrán, respectivamente, de acuerdo entre sí para hacer el nombramiento.

Estos peritos deberán ser titulares, a no ser que no los hubiere de esta clase en el partido o demarcación, en cuyo caso podrán ser nombrados sin título.

Si la práctica de la diligencia pericial no admitiere espera, se procederá como las circunstancias lo permitan para que el actor y el procesado puedan intervenir en ella.

Artículo 472.

Si las partes hicieren uso de la facultad que se les concede en el artículo anterior, manifestarán al Juez el nombre del perito y ofrecerán al hacer esta manifestación los comprobantes de tener la cualidad de tal perito la persona designada.

En ningún caso podrán hacer uso de dicha facultad después de empezada la operación de reconocimiento.

Artículo 473.

El Juez resolverá sobre la admisión de dichos peritos en la forma determinada en el artículo 470 para las recusaciones.

Artículo 474.

Antes de darse principio al acto pericial, todos los peritos, así los nombrados por el Juez como los que lo hubieren sido por las partes, prestarán juramento, conforme al artículo 434, de proceder bien y fielmente en sus operaciones y de no proponerse otro fin más que el de descubrir y declarar la verdad.

Artículo 475.

El Juez manifestará clara y determinadamente a los peritos el objeto de su informe.

Artículo 476.

Al acto pericial podrán concurrir, en el caso del párrafo segundo del artículo 467, el querellante, si lo hubiere, con su representación, y el procesado con la suya, aun cuando estuviere preso, en cuyo caso adoptará el Juez las precauciones oportunas.

Artículo 477.

El acto pericial será presidido por el Juez instructor o, en virtud de su delegación, por el Juez municipal. Podrá también delegar, en el caso del artículo 353, en un funcionario de Policía judicial.

Asistirá siempre el Secretario que actúe en la causa.

Artículo 478.

El informe pericial comprenderá, si fuere posible:

1.º Descripción de la persona o cosa que sea objeto del mismo en el estado o del modo en que se halle.

El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes.

2.º Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.

3.º Las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

Artículo 479.

Si los peritos tuvieren necesidad de destruir o alterar los objetos que analicen, deberá conservarse, a ser posible, parte de ellos a disposición del Juez, para que, en caso necesario, pueda hacerse nuevo análisis.

Artículo 480.

Las partes que asistieren a las operaciones o reconocimientos podrán someter a los peritos las observaciones que estimen convenientes, haciéndose constar todas en la diligencia.

Artículo 481.

Hecho el reconocimiento, podrán los peritos, si lo pidieran, retirarse por el tiempo absolutamente preciso al sitio que el Juez les señale para deliberar y redactar las conclusiones.

Artículo 482.

Si los peritos necesitaren descanso, el Juez o el funcionario que le represente podrá concederles para ello el tiempo necesario.

También podrá suspender la diligencia hasta otra hora u otro día, cuando lo exigiere su naturaleza.

En este caso, el Juez o quien lo represente adoptará las precauciones convenientes para evitar cualquier alteración en la materia de la diligencia pericial.

Artículo 483.

El Juez podrá, por su propia iniciativa o por reclamación de las partes presentes o de sus defensores, hacer a los peritos, cuando produzcan sus conclusiones, las preguntas que estime pertinentes y pedirles las aclaraciones necesarias.

Las contestaciones de los peritos se considerarán como parte de su informe.

Artículo 484.

Si los peritos estuviesen discordes y su número fuere par, nombrará otro el Juez.

Con intervención del nuevamente nombrado, se repetirán, si fuere posible, las operaciones que hubiesen practicado aquéllos, y se ejecutarán las demás que parecieren oportunas.

Si no fuere posible la repetición de las operaciones ni la práctica de otras nuevas, la intervención del perito últimamente nombrado se limitará a deliberar con los demás, con vista de las diligencias de reconocimiento practicadas, y a formular luego con quien estuviere conforme, o separadamente si no lo estuviese con ninguno, sus conclusiones motivadas.

Artículo 485.

El Juez facilitará a los peritos los medios materiales necesarios para practicar la diligencia que les encomiende, reclamándolos de la Administración pública, o dirigiendo a la autoridad correspondiente un aviso previo si existieren preparados para tal objeto, salvo lo dispuesto especialmente en el artículo 362.

[. . .]

TÍTULO VIII

De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución

CAPÍTULO I

De la entrada y registro en lugar cerrado

Artículo 545.

Nadie podrá entrar en el domicilio de un español o extranjero residente en España sin su consentimiento, excepto en los casos y en la forma expresamente previstos en las leyes.

Artículo 546.

El Juez o Tribunal que conociere de la causa podrá decretar la entrada y registro, de día o de noche, en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación.

Artículo 547.

Se reputarán edificios o lugares públicos para la observancia de lo dispuesto en este capítulo:

1.º Los que estuvieren destinados a cualquier servicio oficial, militar o civil del Estado, de la Provincia o del Municipio, aunque habiten allí los encargados de dicho servicio o los de la conservación y custodia del edificio o lugar.

2.º Los que estuvieren destinados a cualquier establecimiento de reunión o recreo, fueren o no lícitos.

3.º Cualesquiera otros edificios o lugares cerrados que no constituyeren domicilio de un particular con arreglo a lo dispuesto en el artículo 554.

4.º Los buques del Estado.

Artículo 548.

El Juez necesitará para la entrada y registro en el Palacio de cualquiera de los Cuerpos Colegisladores la autorización del Presidente respectivo.

Artículo 549.

Para la entrada y registro en los templos y demás lugares religiosos bastará pasar recado de atención a las personas a cuyo cargo estuvieren.

Artículo 550.

Podrá asimismo el Juez instructor ordenar en los casos indicados en el artículo 546 la entrada y registro, de día o de noche, si la urgencia lo hiciere necesario, en cualquier edificio o lugar cerrado o parte de él, que constituya domicilio de cualquier español o extranjero residente en España, pero precediendo siempre el consentimiento del interesado conforme se previene en el artículo 6.º de la Constitución, o a falta de consentimiento, en virtud de auto motivado, que se notificará a la persona interesada inmediatamente, o lo más tarde dentro de las veinticuatro horas de haberse dictado.

Artículo 551.

Se entenderá que presta su consentimiento aquel que, requerido por quien hubiere de efectuar la entrada y registro para que los permita, ejecuta por su parte los actos necesarios

que de él dependan para que puedan tener efecto, sin invocar la inviolabilidad que reconoce al domicilio el artículo 6.º de la Constitución del Estado(*).

(*)Actualmente art. 18.2 de la Constitución Española.

Artículo 552.

Al practicar los registros deberán evitarse las inspecciones inútiles, procurando no perjudicar ni importunar al interesado más de lo necesario, y se adoptarán todo género de precauciones para no comprometer su reputación, respetando sus secretos si no interesaren a la instrucción.

Artículo 553.

Los Agentes de policía podrán asimismo proceder de propia autoridad a la inmediata detención de las personas cuando haya mandamiento de prisión contra ellas, cuando sean sorprendidas en flagrante delito, cuando un delincuente, inmediatamente perseguido por los Agentes de la autoridad, se oculte o refugie en alguna casa o, en casos de excepcional o urgente necesidad, cuando se trate de presuntos responsables de las acciones a que se refiere el artículo 384 bis, cualquiera que fuese el lugar o domicilio donde se ocultasen o refugiasen, así como al registro que, con ocasión de aquélla, se efectúe en dichos lugares y a la ocupación de los efectos e instrumentos que en ellos se hallasen y que pudieran guardar relación con el delito perseguido.

Del registro efectuado, conforme a lo establecido en el párrafo anterior, se dará cuenta inmediata al Juez competente, con indicación de las causas que lo motivaron y de los resultados obtenidos en el mismo, con especial referencia a las detenciones que, en su caso, se hubieran practicado. Asimismo, se indicarán las personas que hayan intervenido y los incidentes ocurridos.

Artículo 554.

Se reputan domicilio, para los efectos de los artículos anteriores:

1.º Los Palacios Reales, estén o no habitados por el Monarca al tiempo de la entrada o registro.

2.º El edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier español o extranjero residente en España y de su familia.

3.º Los buques nacionales mercantes.

4.º Tratándose de personas jurídicas imputadas, el espacio físico que constituya el centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento dependiente, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros.

Artículo 555.

Para registrar en el Palacio en que se halle residiendo el Monarca, solicitará el Juez real licencia por conducto del Mayordomo Mayor de Su Majestad.

Artículo 556.

En los Sitios Reales en que no se hallare el Monarca al tiempo del registro, será necesaria la licencia del Jefe o empleado del servicio de Su Majestad que tuviera a su cargo la custodia del edificio, o la del que haga sus veces cuando se solicitare, si estuviere ausente.

Artículo 557.

(Anulado)

Artículo 558.

El auto de entrada y registro en el domicilio de un particular será siempre fundado, y el Juez expresará en él concretamente el edificio o lugar cerrado en que haya de verificarse, si tendrá lugar tan sólo de día y la Autoridad o funcionario que los haya de practicar.

Artículo 559.

Para la entrada y registro en los edificios destinados a la habitación u oficina de los representantes de naciones extranjeras acreditados cerca del Gobierno de España, les pedirá su venia el Juez, por medio de atento oficio, en el que les rogará que contesten en el término de doce horas.

Artículo 560.

Si transcurriese este término sin haberlo hecho, o si el representante extranjero denegare la venia, el Juez lo comunicará inmediatamente al Ministerio de Gracia y Justicia, empleando para ello el telégrafo, si lo hubiere. Entre tanto que el Ministro no le comunique su resolución, se abstendrá de entrar y registrar en el edificio; pero adoptará las medidas de vigilancia a que se refiere el artículo 567.

Artículo 561.

En los buques extranjeros de guerra, la falta de autorización del Comandante se suplirá por la del Embajador o Ministro de la nación a que pertenezcan.

Artículo 562.

Se podrá entrar en las habitaciones de los Cónsules extranjeros y en sus oficinas pasándoles previamente recado de atención y observando las formalidades prescritas en la Constitución del Estado y en las leyes.

Artículo 563.

Si el edificio o lugar cerrado estuviese en el territorio propio del Juez instructor, podrá encomendar la entrada y registro al Juez municipal del territorio en que el edificio o lugar cerrado radiquen, o a cualquier Autoridad o agente de Policía judicial. Si el que lo hubiese ordenado fuere el Juez municipal, podrá encomendarlo también a dichas Autoridades o agentes de Policía judicial.

Cuando el edificio o lugar cerrado estuviere fuera del territorio del Juez, encomendará éste la práctica de las operaciones al Juez de su propia categoría del territorio en que aquéllos radiquen, el cual, a su vez, podrá encomendarlas a las Autoridades o agentes de Policía judicial.

Artículo 564.

Si se tratare de un edificio o lugar público comprendido en los números 1.º y 3.º del artículo 547, el Juez oficiará a la Autoridad o Jefe de que aquéllos dependan en la misma población.

Si éste no contestare en el término que se le fije en el oficio, se notificará el auto en que se disponga la entrada y registro al encargado de la conservación o custodia del edificio o lugar en que se hubiere de entrar y registrar.

Si se tratare de buques del Estado, las comunicaciones se dirigirán a los Comandantes respectivos.

Artículo 565.

Cuando el edificio o lugar fueren de los comprendidos en el número 2.º del artículo 547, la notificación se hará a la persona que se halle al frente del establecimiento de reunión o recreo, o a quien haga sus veces si aquél estuviere ausente.

Artículo 566.

Si la entrada y registro se hubieren de hacer en el domicilio de un particular, se notificará el auto a éste; y si no fuere habido a la primera diligencia en busca, a su encargado.

Si no fuere tampoco habido el encargado, se hará la notificación a cualquier otra persona mayor de edad que se hallare en el domicilio, prefiriendo para esto a los individuos de la familia del interesado.

Si no se halla a nadie, se hará constar por diligencia, que se extenderá con asistencia de dos vecinos, los cuales deberán firmarla.

Artículo 567.

Desde el momento en que el Juez acuerde la entrada y registro en cualquier edificio o lugar cerrado, adoptará las medidas de vigilancia convenientes para evitar la fuga del procesado o la sustración de los instrumentos, efectos del delito, libros, papeles o cualesquiera otras cosas que hayan de ser objeto del registro.

Artículo 568.

Practicadas las diligencias que se establecen en los artículos anteriores, se procederá a la entrada y registro, empleando para ello, si fuere necesario, el auxilio de la fuerza.

Artículo 569.

El registro se hará a presencia del interesado o de la persona que legitimamente le represente.

Si aquél no fuere habido o no quisiese concurrir ni nombrar representante, se practicará a presencia de un individuo de su familia mayor de edad.

Si no le hubiere, se hará a presencia de dos testigos, vecinos del mismo pueblo.

El registro se practicará siempre en presencia del Secretario del Juzgado o Tribunal que lo hubiera autorizado, o del Secretario del servicio de guardia que le sustituya, quien levantará acta del resultado, de la diligencia y de sus incidencias y que será firmada por todos los asistentes. No obstante, en caso de necesidad, el Secretario judicial podrá ser sustituido en la forma prevista en la Ley Orgánica del Poder Judicial.

La resistencia del interesado, de su representante, de los individuos de la familia y de los testigos a presenciar el registro producirá la responsabilidad declarada en el Código Penal a los reos del delito de desobediencia grave a la Autoridad, sin perjuicio de que la diligencia se practique.

Si no se encontrasen las personas u objetos que se busquen ni apareciesen indicios sospechosos, se expedirá una certificación del acta a la parte interesada si la reclamare.

Artículo 570.

Cuando el registro se practique en el domicilio de un particular y expire el día sin haberse terminado, el que lo haga requerirá al interesado o a su representante, si estuviere presente, para que permita la continuación durante la noche. Si se opusiere, se suspenderá la diligencia, salvo lo dispuesto en los artículos 546 y 550, cerrando y sellando el local o los muebles en que hubiere de continuarse, en cuanto esta precaución se considere necesaria para evitar la fuga de la persona o la sustracción de las cosas que se buscaren.

Prevendrá asimismo el que practique el registro a los que se hallen en el edificio o lugar de la diligencia que no levanten los sellos, ni violenten las cerraduras, ni permitan que lo hagan otras personas, bajo la responsabilidad establecida en el Código Penal.

Artículo 571.

El registro no se suspenderá sino por el tiempo en que no fuere posible continuarle, y se adoptarán, durante la suspensión, las medidas de vigilancia a que se refiere el artículo 567.

Artículo 572.

En la diligencia de entrada y registro en lugar cerrado, se expresarán los nombres del Juez, o de su delegado, que la practique y de las demás personas que intervengan, los incidentes ocurridos, la hora en que se hubiese principiado y concluido la diligencia, y la relación del registro por el orden con que se haga, así como los resultados obtenidos.

CAPÍTULO II

Del registro de libros y papeles

Artículo 573.

No se ordenará el registro de los libros y papeles de contabilidad del procesado o de otra persona sino cuando hubiere indicios graves de que de esta diligencia resultará el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

Artículo 574.

El Juez ordenará recoger los instrumentos y efectos del delito y también los libros, papeles o cualesquiera otras cosas que se hubiesen encontrado, si esto fuere necesario para el resultado del sumario.

Los libros y papeles que se recojan serán foliados, sellados y rubricados en todas sus hojas por el Secretario judicial, bajo su responsabilidad.

Artículo 575.

Todos están obligados a exhibir los objetos y papeles que se sospeche puedan tener relación con la causa.

Si el que los retenga se negare a su exhibición, será corregido con multa de 125 a 500 pesetas; y cuando insistiera en su negativa, si el objeto o papel fueren de importancia y la índole del delito lo aconseje, será procesado como autor del de desobediencia a la Autoridad, salvo si mereciera la calificación legal de encubridor o receptador.

Artículo 576.

Será aplicable al registro de papeles y efectos lo establecido en los artículos 552 y 569.

Artículo 577.

Si para determinar sobre la necesidad de recoger las cosas que se hubiesen encontrado en el registro fuere necesario algún reconocimiento pericial, se acordará en el acto por el Juez, en la forma establecida en el capítulo VII del título V.

Artículo 578.

Si el libro que haya de ser objeto del registro fuere el protocolo de un Notario, se procederá con arreglo a lo dispuesto en la Ley del Notariado.

Si se tratare de un libro del Registro de la Propiedad, se estará a lo ordenado en la Ley Hipotecaria.

Si se tratare de un libro del Registro Civil o Mercantil se estará a lo que se disponga en la Ley y Reglamentos relativos a estos servicios.

CAPÍTULO III

De la detención y apertura de la correspondencia escrita y telegráfica

Artículo 579. *De la correspondencia escrita o telegráfica.*

1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o

examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo.

2. El juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos.
3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.
4. No se requerirá autorización judicial en los siguientes casos:

a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido.
b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.
c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío.

5. La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 579 bis. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*

1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.
3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.

Artículo 580.

Es aplicable a la detención de la correspondencia lo dispuesto en los artículos 563 y 564.
Podrá también encomendarse la práctica de esta operación al Administrador de Correos y Telégrafos o Jefe de la oficina en que la correspondencia deba hallarse.

Artículo 581.

El empleado que haga la detención remitirá inmediatamente la correspondencia detenida al Juez instructor de la causa.

Artículo 582.

Podrá asimismo el Juez ordenar que por cualquier Administración de Telégrafos se le faciliten copias de los telegramas por ella transmitidos, si pudieran contribuir al esclarecimiento de los hechos de la causa.

Artículo 583.

El auto motivado acordando la detención y registro de la correspondencia o la entrega de copias de telegramas transmitidos determinará la correspondencia que haya de ser detenida o registrada, o los telegramas cuyas copias hayan de ser entregadas, por medio de la designación de las personas a cuyo nombre se hubieran expedido, o por otras circunstancias igualmente concretas.

Artículo 584.

Para la apertura y registro de la correspondencia postal será citado el interesado.

Éste o la persona que designe podrá presenciar la operación.

Artículo 585.

Si el procesado estuviere en rebeldía, o si citado para la apertura no quisiere presenciarla ni nombrar persona para que lo haga en su nombre, el Juez instructor procederá, sin embargo, a la apertura de dicha correspondencia.

Artículo 586.

La operación se practicará abriendo el Juez por sí mismo la correspondencia, y después de leerla para sí apartará la que haga referencia a los hechos de la causa y cuya conservación considere necesaria.

Los sobres y hojas de esta correspondencia, después de haber tomado el mismo Juez las notas necesarias para la práctica de otras diligencias de investigación a que la correspondencia diere motivo, se rubricarán por el Secretario judicial y se sellarán con el sello del Juzgado, encerrándolo todo después en otro sobre, al que se pondrá el rótulo necesario, conservándose durante el sumario, también bajo responsabilidad del Secretario judicial.

Este pliego podrá abrirse cuantas veces el Juez lo considere preciso, citando previamente al interesado.

Artículo 587.

La correspondencia que no se relacione con la causa será entregada en el acto al procesado o a su representante.

Si aquél estuviere en rebeldía, se entregará cerrada a un individuo de su familia mayor de edad.

Si no fuere conocido ningún pariente del procesado, se conservará dicho pliego cerrado bajo la responsabilidad del Secretario judicial hasta que haya persona a quien entregarlo, según lo dispuesto en este artículo.

Artículo 588.

La apertura de la correspondencia se hará constar por diligencia, en la que se referirá cuanto en aquélla hubiese ocurrido.

Esta diligencia será firmada por el Juez instructor, el Secretario y demás asistentes.

CAPÍTULO IV

Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos

Artículo 588 bis a. *Principios rectores.*

1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Artículo 588 bis b. *Solicitud de autorización judicial.*

1. El juez podrá acordar las medidas reguladas en este capítulo de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial.

2. Cuando el Ministerio Fiscal o la Policía Judicial soliciten del juez de instrucción una medida de investigación tecnológica, la petición habrá de contener:

1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4.º La extensión de la medida con especificación de su contenido.

5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6.º La forma de ejecución de la medida.

7.º La duración de la medida que se solicita.

8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Artículo 588 bis c. *Resolución judicial.*

1. El juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado, oído el Ministerio Fiscal. Esta resolución se dictará en el plazo máximo de veinticuatro horas desde que se presente la solicitud.

2. Siempre que resulte necesario para resolver sobre el cumplimiento de alguno de los requisitos expresados en los artículos anteriores, el juez podrá requerir, con interrupción del plazo a que se refiere el apartado anterior, una ampliación o aclaración de los términos de la solicitud.

3. La resolución judicial que autorice la medida concretará al menos los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Artículo 588 bis d. *Secreto.*

La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 588 bis e. *Duración.*

1. Las medidas reguladas en el presente capítulo tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.

2. La medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron.

3. Transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos.

Artículo 588 bis f. *Solicitud de prórroga.*

1. La solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido. Deberá incluir en todo caso:

a) Un informe detallado del resultado de la medida.

b) Las razones que justifiquen la continuación de la misma.

2. En el plazo de los dos días siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante auto motivado. Antes de dictar la resolución podrá solicitar aclaraciones o mayor información.

3. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada.

Artículo 588 bis g. *Control de la medida.*

La Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma.

Artículo 588 bis h. *Afectación de terceras personas.*

Podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Artículo 588 bis i. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*

El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularan con arreglo a lo dispuesto en el artículo 579 bis.

Artículo 588 bis j. *Cese de la medida.*

El juez acordará el cese de la medida cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos, y, en todo caso, cuando haya transcurrido el plazo para el que hubiera sido autorizada.

Artículo 588 bis k. *Destrucción de registros.*

1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial.
2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.
3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.

CAPÍTULO V

La interceptación de las comunicaciones telefónicas y telemáticas

Sección 1.ª Disposiciones generales

Artículo 588 ter a. *Presupuestos.*

La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Artículo 588 ter b. *Ámbito.*

1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.
2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como

emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.

También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

Artículo 588 ter c. *Afectación a tercero.*

Podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que:

1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o

2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Artículo 588 ter d. *Solicitud de autorización judicial.*

1. La solicitud de autorización judicial deberá contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,

b) la identificación de la conexión objeto de la intervención o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

2. Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:

a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.

b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

c) La localización geográfica del origen o destino de la comunicación.

d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.

3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

Artículo 588 ter e. *Deber de colaboración.*

1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados

a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.

2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia.

Artículo 588 ter f. *Control de la medida.*

En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Artículo 588 ter g. *Duración.*

La duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Artículo 588 ter h. *Solicitud de prórroga.*

Para la fundamentación de la solicitud de la prórroga, la Policía Judicial aportará, en su caso, la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.

Antes de dictar la resolución, el juez podrá solicitar aclaraciones o mayor información, incluido el contenido íntegro de las conversaciones intervenidas.

Artículo 588 ter i. *Acceso de las partes a las grabaciones.*

1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso.

2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

Sección 2.ª Incorporación al proceso de datos electrónicos de tráfico o asociados

Artículo 588 ter j. *Datos obrantes en archivos automatizados de los prestadores de servicios.*

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

Artículo 588 ter k. *Identificación mediante número IP.*

Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Artículo 588 ter l. *Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.*

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Artículo 588 ter m. *Identificación de titulares o terminales o dispositivos de conectividad.*

Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones

o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

CAPÍTULO VI

Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Artículo 588 quater a. *Grabación de las comunicaciones orales directas.*

1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.

Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.

2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.

3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.

Artículo 588 quater b. *Presupuestos.*

1. La utilización de los dispositivos a que se refiere el artículo anterior ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación.

2. Solo podrá autorizarse cuando concurran los requisitos siguientes:

a) Que los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

b) Que pueda racionalmente preverse que la utilización de los dispositivos aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor.

Artículo 588 quater c. *Contenido de la resolución judicial.*

La resolución judicial que autorice la medida, deberá contener, además de las exigencias reguladas en el artículo 588 bis c, una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia.

Artículo 588 quater d. *Control de la medida.*

En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición de la autoridad judicial el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.

El informe identificará a todos los agentes que hayan participado en la ejecución y seguimiento de la medida.

Artículo 588 quater e. *Cese.*

Cesada la medida por alguna de las causas previstas en el artículo 588 bis j, la grabación de conversaciones que puedan tener lugar en otros encuentros o la captación de imágenes de tales momentos exigirán una nueva autorización judicial.

CAPÍTULO VII

Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

Artículo 588 quinquies a. *Captación de imágenes en lugares o espacios públicos.*

1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

2. La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.

Artículo 588 quinquies b. *Utilización de dispositivos o medios técnicos de seguimiento y localización.*

1. Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización.

2. La autorización deberá especificar el medio técnico que va a ser utilizado.

3. Los prestadores, agentes y personas a que se refiere el artículo 588 ter e están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia.

4. Cuando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso.

Artículo 588 quinquies c. *Duración de la medida.*

1. La medida de utilización de dispositivos técnicos de seguimiento y localización prevista en el artículo anterior tendrá una duración máxima de tres meses a partir de la fecha de su autorización. Excepcionalmente, el juez podrá acordar prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida.

2. La Policía Judicial entregará al juez los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones.

3. La información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida.

CAPÍTULO VIII

Registro de dispositivos de almacenamiento masivo de información

Artículo 588 sexies a. *Necesidad de motivación individualizada.*

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Artículo 588 sexies b. *Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.*

La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización.

Artículo 588 sexies c. *Autorización judicial.*

1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se

ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

CAPÍTULO IX

Registros remotos sobre equipos informáticos

Artículo 588 septies a. *Presupuestos.*

1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

Artículo 588 septies b. *Deber de colaboración.*

1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

4. Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e.

Artículo 588 septies c. *Duración.*

La medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

CAPÍTULO X

Medidas de aseguramiento

Artículo 588 octies. *Orden de conservación de datos.*

El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes.

Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.

El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e.

[. . .]

TÍTULO III

De la celebración del juicio oral

[. . .]

CAPÍTULO III

Del modo de practicar las pruebas durante el juicio oral

[. . .]

Sección 3.ª Del informe pericial

Artículo 723.

Los peritos podrán ser recusados por las causas y en la forma prescrita en los artículos 468, 469 y 470.

La sustanciación de los incidentes de recusación tendrá lugar precisamente en el tiempo que media desde la admisión de las pruebas propuestas por las partes hasta la apertura de las sesiones.

Artículo 724.

Los peritos que no hayan sido recusados serán examinados juntos cuando deban declarar sobre unos mismos hechos, y contestarán a las preguntas y repreguntas que las partes les dirijan.

Artículo 725.

Si para contestarlas considerasen necesaria la práctica de cualquier reconocimiento, harán éste, acto continuo, en el local de la misma audiencia si fuere posible.

En otro caso se suspenderá la sesión por el tiempo necesario, a no ser que puedan continuar practicándose otras diligencias de prueba entre tanto que los peritos verifican el reconocimiento.

Sección 4.ª De la prueba documental y de la inspección ocular

Artículo 726.

El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad.

Artículo 727.

Para la prueba de inspección ocular que no se haya practicado antes de la apertura de las sesiones, si el lugar que deba ser inspeccionado se hallase en la capital, se constituirá en él el Tribunal con las partes, y el Secretario extenderá diligencia expresiva del lugar o cosa inspeccionada, haciendo constar en ella las observaciones de las partes y demás incidentes que ocurran.

Si el lugar estuviere fuera de la capital, se constituirá en él con las partes el individuo del Tribunal que el Presidente designe, practicándose las diligencias en la forma establecida en el párrafo anterior.

En todo lo demás se estará, en cuanto fuere necesario, a lo dispuesto en el título V, capítulo I del libro II.

[. . .]

TÍTULO II

Del procedimiento abreviado

[. . .]

CAPÍTULO II

De las actuaciones de la Policía Judicial y del Ministerio Fiscal

Artículo 769.

Sin perjuicio de lo establecido en el Título III del Libro II de esta Ley, tan pronto como tenga conocimiento de un hecho que revista caracteres de delito, la Policía judicial observará las reglas establecidas en este capítulo.

Artículo 770.

La Policía Judicial acudirá de inmediato al lugar de los hechos y realizará las siguientes diligencias:

1.ª Requerirá la presencia de cualquier facultativo o personal sanitario que fuere habido para prestar, si fuere necesario, los oportunos auxilios al ofendido. El requerido, aunque sólo lo fuera verbalmente, que no atienda sin justa causa el requerimiento será sancionado con una multa de 500 a 5.000 euros, sin perjuicio de la responsabilidad criminal en que hubiera podido incurrir.

2.ª Acompañará al acta de constancia fotografías o cualquier otro soporte magnético o de reproducción de la imagen, cuando sea pertinente para el esclarecimiento del hecho punible y exista riesgo de desaparición de sus fuentes de prueba.

3.ª Recogerá y custodiará en todo caso los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, para ponerlos a disposición de la autoridad judicial.

4.ª Si se hubiere producido la muerte de alguna persona y el cadáver se hallare en la vía pública, en la vía férrea o en otro lugar de tránsito, lo trasladará al lugar próximo que resulte más idóneo dentro de las circunstancias, restableciendo el servicio interrumpido y dando cuenta de inmediato a la autoridad judicial. En las situaciones excepcionales en que haya de adoptarse tal medida de urgencia, se reseñará previamente la posición del interfecto, obteniéndose fotografías y señalando sobre el lugar la situación exacta que ocupaba.

5.ª Tomará los datos personales y dirección de las personas que se encuentren en el lugar en que se cometió el hecho, así como cualquier otro dato que ayude a su identificación y localización, tales como lugar habitual de trabajo, números de teléfono fijo o móvil, número de fax o dirección de correo electrónico.

6.ª Intervendrá, de resultar procedente, el vehículo y retendrá el permiso de circulación del mismo y el permiso de conducir de la persona a la que se impute el hecho.

Artículo 771.

En el tiempo imprescindible y, en todo caso, durante el tiempo de la detención, si la hubiere, la Policía Judicial practicará las siguientes diligencias:

1.ª Cumplirá con los deberes de información a las víctimas que prevé la legislación vigente. En particular, informará al ofendido y al perjudicado por el delito de forma escrita de los derechos que les asisten de acuerdo con lo establecido en los artículos 109 y 110. Se instruirá al ofendido de su derecho a mostrarse parte en la causa sin necesidad de formular querella y, tanto al ofendido como al perjudicado, de su derecho a nombrar Abogado o instar el nombramiento de Abogado de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita, de su derecho a, una vez personados en la causa, tomar conocimiento de lo actuado, sin perjuicio de lo dispuesto en los artículos 301 y 302, e instar lo que a su derecho convenga. Asimismo, se les informará de que, de no personarse en la causa y no hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere.

La información de derechos al ofendido o perjudicado regulada en este artículo, cuando se refiera a los delitos contra la propiedad intelectual o industrial, y, en su caso, su citación o emplazamiento en los distintos trámites del proceso, se realizará a aquellas personas, entidades u organizaciones que ostenten la representación legal de los titulares de dichos derechos.

2.ª Informará en la forma más comprensible al investigado no detenido de cuáles son los hechos que se le atribuyen y de los derechos que le asisten. En particular, le instruirá de los derechos reconocidos en los apartados a), b), c) y e) del artículo 520.2.

Artículo 772.

1. Los miembros de la Policía Judicial requerirán el auxilio de otros miembros de las Fuerzas y Cuerpos de Seguridad cuando fuera necesario para el desempeño de las funciones que por esta Ley se les encomiendan.

2. La Policía extenderá el atestado de acuerdo con las normas generales de esta Ley y lo entregará al Juzgado competente, pondrá a su disposición a los detenidos, si los hubiere, y remitirá copia al Ministerio Fiscal.

Artículo 773.

1. El Fiscal se constituirá en las actuaciones para el ejercicio de las acciones penal y civil conforme a la Ley. Velará por el respeto de las garantías procesales del investigado o

encausado y por la protección de los derechos de la víctima y de los perjudicados por el delito.

En este procedimiento corresponde al Ministerio Fiscal, de manera especial, impulsar y simplificar su tramitación sin merma del derecho de defensa de las partes y del carácter contradictorio del mismo, dando a la Policía Judicial instrucciones generales o particulares para el más eficaz cumplimiento de sus funciones, interviniendo en las actuaciones, aportando los medios de prueba de que pueda disponer o solicitando del Juez de Instrucción la práctica de los mismos, así como instar de éste la adopción de medidas cautelares o su levantamiento y la conclusión de la investigación tan pronto como estime que se han practicado las actuaciones necesarias para resolver sobre el ejercicio de la acción penal.

El Fiscal General del Estado impartirá cuantas órdenes e instrucciones estime convenientes respecto a la actuación del Fiscal en este procedimiento, y en especial, respecto a la aplicación de lo dispuesto en el apartado 1 del artículo 780.

Tan pronto como el Juez ordene la incoación del procedimiento para las causas ante el Tribunal del Jurado, el Secretario judicial lo pondrá en conocimiento del Ministerio Fiscal, quien comparecerá e intervendrá en cuantas actuaciones se lleven a cabo ante aquél.

2. Cuando el Ministerio Fiscal tenga noticia de un hecho aparentemente delictivo, bien directamente o por serle presentada una denuncia o atestado, informará a la víctima de los derechos recogidos en la legislación vigente; efectuará la evaluación y resolución provisionales de las necesidades de la víctima de conformidad con lo dispuesto en la legislación vigente y practicará él mismo u ordenará a la Policía Judicial que practique las diligencias que estime pertinentes para la comprobación del hecho o de la responsabilidad de los partícipes en el mismo. El Fiscal decretará el archivo de las actuaciones cuando el hecho no revista los caracteres de delito, comunicándolo con expresión de esta circunstancia a quien hubiere alegado ser perjudicado u ofendido, a fin de que pueda reiterar su denuncia ante el Juez de Instrucción. En otro caso instará del Juez de Instrucción la incoación del procedimiento que corresponda con remisión de lo actuado, poniendo a su disposición al detenido, si lo hubiere, y los efectos del delito.

El Ministerio Fiscal podrá hacer comparecer ante sí a cualquier persona en los términos establecidos en la ley para la citación judicial, a fin de recibirle declaración, en la cual se observarán las mismas garantías señaladas en esta Ley para la prestada ante el Juez o Tribunal.

Cesará el Fiscal en sus diligencias tan pronto como tenga conocimiento de la existencia de un procedimiento judicial sobre los mismos hechos.

[. . .]

TÍTULO V

Del procedimiento por delitos cometidos por medio de la imprenta, el grabado u otro medio mecánico de publicación

Artículo 816.

Inmediatamente que se dé principio a un procedimiento por delito cometido por medio de la imprenta, el grabado u otro medio mecánico de publicación, el Juez o Tribunal acordará el secuestro de los ejemplares del impreso o de la estampa donde quiera que se hallaren y del molde de ésta.

Se procederá, asimismo, inmediatamente a averiguar quién haya sido el autor real del escrito o estampa con cuya publicación se hubiese cometido el delito.

Artículo 817.

Si el escrito o estampa se hubiese publicado en periódico, bien en el texto del mismo, bien en hoja aparte, se tomará declaración para averiguar quién haya sido el autor al Director o redactores de aquél y al Jefe o Regente del establecimiento tipográfico en que se haya hecho la impresión o grabado.

Para ello se reclamará el original de cualquiera de las personas que lo tenga en su poder, la cual, si no lo pusiere a disposición del Juez, manifestará la persona a quien lo haya entregado.

Artículo 818.

Si el delito se hubiese cometido por medio de la publicación de un escrito o de una estampa sueltos, se tomará la declaración expresada en el artículo anterior al Jefe y dependientes del establecimiento en que se haya hecho la impresión o estampación.

Artículo 819.

Cuando no pudiere averiguarse quién sea el autor real del escrito o estampa, o cuando por hallarse domiciliado en el extranjero o por cualquier otra causa de las especificadas en el Código Penal no pudiere ser perseguido, se dirigirá el procedimiento contra las personas subsidiariamente responsables, por el orden establecido en el artículo respectivo del expresado Código.

Artículo 820.

No será bastante la confesión de un supuesto autor para que se le tenga como tal y para que no se dirija el procedimiento contra otras personas, si de las circunstancias de aquél o de las del delito resultaren indicios bastantes para creer que el confeso no fue el autor real del escrito o estampa publicados.

Pero una vez dictada sentencia firme en contra de los subsidiariamente responsables, no se podrá abrir nuevo procedimiento contra el responsable principal si llegare a ser conocido.

Artículo 821.

Si durante el curso de la causa apareciere alguna persona que, por el orden establecido en el artículo respectivo del Código Penal, deba responder criminalmente del delito antes que el procesado, se sobreseerá la causa respecto a éste, dirigiéndose el procedimiento contra aquélla.

Artículo 822.

No se considerarán como instrumentos o efectos del delito más que los ejemplares impresos del escrito o estampa y el molde de ésta.

Artículo 823.

Unidos a la causa el impreso, grabado u otro medio mecánico de publicación que haya servido para la comisión del delito, y averiguado el autor o la persona subsidiariamente responsable, se dará por terminado el sumario.

Artículo 823 bis.

Las normas del presente título serán también aplicables al enjuiciamiento de los delitos cometidos a través de medios sonoros o fotográficos, difundidos por escrito, radio, televisión, cinematógrafo u otros similares.

Los Jueces, al iniciar el procedimiento, podrán acordar, según los casos, el secuestro de la publicación o la prohibición de difundir o proyectar el medio a través del cual se produjo la actividad delictiva. Contra dicha resolución podrá interponerse directamente recurso de apelación, que deberá ser resuelto en el plazo de cinco días.

[. . .]

§ 41

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Jefatura del Estado
«BOE» núm. 298, de 14 de diciembre de 1999
Última modificación: 5 de marzo de 2011
Referencia: BOE-A-1999-23750

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de

su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. *Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. *Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. *Acceso a los datos por cuenta de terceros.*

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. *Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. *Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. *Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. *Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. *Tutela de los derechos.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia

de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. *Derecho a indemnización.*

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. *Creación, modificación o supresión.*

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. *Comunicación de datos entre Administraciones públicas.*

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo **cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o** cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Téngase en cuenta que se declara la inconstitucionalidad y nulidad del inciso destacado del apartado 1 por Sentencia del TC 292/2000, de 30 de noviembre. Ref. BOE-T-2001-332

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado **impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas** o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales **o administrativas**.

Téngase en cuenta que se declara la inconstitucionalidad y nulidad de los incisos destacados del apartado 1 por Sentencia del TC 292/2000, de 30 de noviembre. Ref. BOE-T-2001-332

2. **(Anulado)**

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. *Creación.*

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley

deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento.

Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. *Norma general.*

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.

Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada

puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. *El Director.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. *Funciones.*

1. Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Artículo 38. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. *El Registro General de Protección de Datos.*

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de

Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. *Potestad de inspección.*

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. *Órganos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. *Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. *Responsables.*

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de titularidad pública se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en los artículos 46 y 48 de la presente Ley.

Artículo 44. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:

a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.
b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.
c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.
b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.
c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.
e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.
h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
j) La obstrucción al ejercicio de la función inspectora.
k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa o fraudulenta.
b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
c) No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Artículo 45. *Tipo de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.
2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.

b) El volumen de los tratamientos efectuados.

c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

d) El volumen de negocio o actividad del infractor.

e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

f) El grado de intencionalidad.

g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

6. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

7. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

8. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta

resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. *Procedimiento sancionador.*

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.

Artículo 49. *Potestad de inmovilización de ficheros.*

En los supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Ficheros preexistentes.*

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor.

En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. *Ficheros y Registro de Población de las Administraciones públicas.*

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del artículo 112.4 de la Ley General Tributaria.*

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

"4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado.

En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal."

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora.

La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado."

Disposición transitoria primera. *Tratamientos creados por Convenios internacionales.*

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. *Utilización del censo promocional.*

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas.

El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. *Subsistencia de normas preexistentes.*

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. *Habilitación para el desarrollo reglamentario.*

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Preceptos con carácter de Ley ordinaria.*

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el "Boletín Oficial del Estado".

§ 42

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo

deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre

que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.

3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación

directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

> Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o

comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este

precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo

ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
f) Los órganos responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.
3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.
2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.
3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su

finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.
2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.
3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.
4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
b) Las previsiones específicas para la aplicación de los principios de protección de datos.
c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:
a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.
2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.
b) La identificación de las categorías de cesionarios o importadores de los datos.
c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.
d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y

reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el

sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de

medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.

2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.

3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no

existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.
b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.
d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.
e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.
f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.
g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.
2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.
2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.
2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.
2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.
b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.
c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.
d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.