BORRADOR DE ANTEPROYECTO DE LEY SOBRE LA SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

EXPOSICIÓN DE MOTIVOS

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y en la sociedad con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.

El carácter transversal e interconectado de las tecnologías de la información, que también caracteriza a sus amenazas y riesgos, limita la eficacia de las medidas que se emplean para contrarrestarlos, cuando éstas se toman de modo aislado. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos sectoriales afectados.

Por tanto, es oportuno establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

II

Con este propósito se dicta esta ley, que transpone la 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. Pero, se apoya igualmente en las normas, en los instrumentos de respuesta a incidentes y en los órganos de coordinación estatal existentes en esta materia, lo que, junto a las razones señaladas en el apartado I, justifica que su contenido trascienda el de la propia Directiva.

La ley se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Su ámbito de aplicación se extiende a servicios tanto excluidos como no expresamente incluidos en la Directiva, para darle a esta ley un enfoque global, aunque se preserva su legislación específica.

En el caso de los servicios de explotación de las redes y de prestación de servicios de comunicaciones electrónicas, así como de los servicios electrónicos de confianza, la ley se aplicará en lo que respecta a los operadores críticos.

La ley se aplicará, así mismo, a los proveedores de determinados servicios digitales. La Directiva los somete a un régimen de armonización máxima, equivalente a un reglamento, pues se considera que su regulación a escala nacional no sería efectiva por tener un carácter intrínsecamente transnacional. La función de las autoridades nacionales se limita por tanto, a supervisar su aplicación por los proveedores establecidos en su país, y coordinarse con las autoridades correspondientes de otros países de la Unión Europea.

Siguiendo la Directiva, la ley identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores así como a los principales operadores que prestan dichos servicios, que son, en definitiva, los destinatarios de esta ley.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilicen, aunque su gestión esté externalizada. Las obligaciones de seguridad que asuman deberán ser proporcionadas al nivel de riesgo que afronten y estar basadas en una evaluación previa de los mismos. Las normas de desarrollo de esta ley podrán concretar las obligaciones de seguridad exigibles a los operadores de servicios esenciales, incluyendo en su caso las inspecciones a realizar o la participación en actividades y ejercicios de gestión de crisis.

La ley prevé, así mismo, que los operadores de servicios esenciales y los proveedores de servicios digitales notifiquen los incidentes significativos que sufran en las redes y servicios de información que emplean para la prestación de los servicios esenciales y digitales, y perfila el procedimiento de notificación.

La notificación de incidentes forma parte de la cultura de gestión de riesgos que la Directiva y la ley fomentan. Por ello, la ley protege a la entidad notificante y a todo empleado que informe sobre incidentes ocurridos; se reserva la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permite la notificación de incidentes cuando no sea obligada su comunicación.

La ley recalca la necesidad de tener en cuenta los estándares europeos e internacionales así como las recomendaciones que emanen de los grupos de cooperación y de la red de CSIRT en el ámbito comunitario con vistas a aplicar las mejores prácticas aprendidas en estos foros y contribuir al impulso del mercado interior y a la participación de nuestras empresas en él.

Con el fin de aumentar su eficacia y al tiempo, reducir las cargas administrativas y económicas que estas obligaciones suponen para las entidades afectadas, esta ley trata de garantizar su coherencia con las que se derivan de la aplicación de otras normativas en materia de seguridad de la información, tanto de carácter horizontal como sectorial, y la coordinación en su aplicación con las autoridades responsables en cada caso.

Respecto a las normas horizontales, destacan los vínculos establecidos con las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, y con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, como normativa especial en materia de seguridad de los sistemas de información del sector público.

Así, se iguala el ámbito de aplicación de esta ley al de la Ley 8/2011, de 28 de abril, añadiendo a los sectores previstos por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los contemplados en esa ley; se toma de ella el concepto de "servicio esencial" y se atribuye a sus órganos colegiados la determinación de los servicios esenciales y de los operadores de servicios esenciales sujetos a la ley. Teniendo en cuenta en cuenta la Ley 36/2015, de 28 de septiembre, se atribuye al Consejo de Seguridad Nacional la función de actuar como punto de contacto con otros países de la Unión Europea y un papel coordinador de la política de ciberseguridad a través de la Estrategia de ciberseguridad nacional.

III

La Estrategia de ciberseguridad nacional, con la que España cuenta desde el año 2013, sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. La Estrategia seguirá desarrollando el marco institucional de la ciberseguridad que esta ley esboza, compuesto por las autoridades públicas competentes y los CSIRT de referencia, por una parte, y la cooperación público-privada, por otra.

Las autoridades competentes ejercerán las funciones de vigilancia derivadas de esta ley, y aplicarán el régimen sancionador, si procede. Así mismo, promoverán el desarrollo mediante reglamentos y documentos técnicos de las obligaciones que la ley impone, en consulta con el sector y con las autoridades que ejerzan competencias por razón de la materia sobre aquel, para evitar crear obligaciones duplicadas, innecesarias o excesivamente onerosas.

Los CSIRT (Computer Security Incident Response Team) son los equipos de respuesta a incidentes que monitorizan las redes para detectar posibles incidentes, difundir alertas sobre ellos y aportar soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT, registrado en EE.UU.

La ley delimita el ámbito funcional de actuación de los CSIRT de referencia previstos en ella. Dichos CSIRT son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a ellos, pero el destinatario de las notificaciones es la autoridad competente respectiva, que tendrá en cuenta esta información para la supervisión de los operadores. En todo caso, el operador es responsable de resolver los incidentes y reponer las redes y sistemas de información afectados a su funcionamiento ordinario.

Se prevé la utilización de una plataforma común para la notificación de incidentes, de tal manera que los operadores no deban efectuar varias notificaciones en función de la

autoridad a la que deban dirigirse. Esta plataforma podrá ser empleada también para la notificación de vulneraciones de la seguridad de datos personales según el 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.

IV

Esta ley consta de siete títulos que contienen, en primer lugar, las definiciones de los términos que se usan a lo largo del texto, la salvaguarda de funciones estatales esenciales, como la seguridad nacional, y otras disposiciones generales. A continuación, se determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten a los que se aplicará la ley. El orden en que se procederá a su identificación por primera vez se establece en la parte final de la ley. El título III recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información que se ha descrito anteriormente. Se dedica un precepto específico a la cooperación entre autoridades públicas, como pilar de un ejercicio adecuado de las diferentes competencias concurrentes sobre la materia.

El título IV se ocupa de las obligaciones de seguridad de los operadores y en él se prevé la aplicación preferente de normas sectoriales que impongan obligaciones equivalentes a las previstas en esta ley, sin perjuicio de la coordinación ejercida por el Consejo de Seguridad Nacional y del deber de cooperación con las autoridades competentes en virtud de esta ley.

En el título V, el más extenso, se regula la notificación de incidentes y se presta atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión. En el título VI, se disponen las potestades de inspección y control de las autoridades competentes, resaltando nuevamente la cooperación con otras autoridades nacionales, y en el título VII, se tipifican las infracciones y sanciones de esta ley. En este aspecto, la ley se decanta por impulsar la subsanación de la infracción antes que su castigo, el cual, si es necesario dispensarlo, será proporcionado pero severo, en línea con lo ordenado por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

La ley se cierra con una parte final, con las disposiciones que resultan preceptivas o convenientes para ordenar ciertas situaciones transitorias.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. La presente ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de esta ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Artículo 2. *Ámbito de aplicación.*

1. Esta ley se aplicará a la prestación de:

   a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

   b) Los servicios digitales, considerados conforme se determina en el artículo 3 e) que sean mercados en línea, motor de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a esta ley:

   a) los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales 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 o actividades.

      Asimismo, esta ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

   b) los proveedores de servicios digitales que tengan su sede social en España así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la 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.

3. Esta ley no se aplicará a:

   a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

Artículo 3. *Definiciones.*

A los efectos de esta ley, se entenderá por:

a) Redes y sistemas de información, cualquiera de los elementos siguientes:

1º) las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;

2º) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales;

3º) los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.° y 2.° anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

b) Seguridad de las redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

c) Servicio esencial: 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, que dependa para su provisión de las redes y sistemas de información.

d) Operador de servicios esenciales: entidad pública o privada que se identifique considerando los criterios establecidos en el artículo 6.2 de esta ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.

h) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

i) Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante este.

j) Representante: persona física o jurídica establecida en la Unión Europea que haya sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea, a la que, en sustitución del proveedor de servicios digitales, pueda dirigirse una autoridad competente nacional o un CSIRT, en relación con las obligaciones que, en virtud de esta ley, tiene el proveedor de servicios digitales.

k) Norma técnica: una norma en el sentido del artículo 2.1 del Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

l) Especificación: una especificación técnica en el sentido del artículo 2.4 del Reglamento (UE) nº 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012.

m) Punto de intercambio de internet («IXP», por sus siglas en inglés de «Internet Exchange Point»): una instalación de la red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de internet. Un IXP permite interconectar sistemas autónomos sin requerir que el tráfico de Internet que pasas entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

n) Sistema de nombres de dominio («DNS», por sus siglas en inglés de «Domain Name System»): sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en internet.

o) Proveedor de servicios de DNS: entidad que presta servicios de DNS en internet.

p) Registro de nombres de dominio de primer nivel: entidad que administra y dirige el registro de nombres de dominio de internet en un dominio específico de primer nivel.

q) Mercado en línea: servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en el sitio web del mercado en línea o en un sitio web de un empresario que utilice servicios informáticos proporcionados por el mercado en línea.

r) Motor de búsqueda en línea: servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

Artículo 4. *Directrices y orientaciones comunitarias.*

En la aplicación de esta ley y en la elaboración de los reglamentos y guías previstos en ella se tendrán en cuenta los actos de ejecución de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016, así como todas las recomendaciones y directrices emanadas del grupo de cooperación establecido por el artículo 11 de la Directiva, y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquella.

Artículo 5. *Salvaguarda de funciones estatales esenciales.*

Lo dispuesto en esta ley se entenderá sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos y el enjuiciamiento de sus autores.

TÍTULO II

Servicios esenciales y servicios digitales

CAPÍTULO I

Servicios esenciales y operadores de servicios esenciales

Artículo 6. *Identificación de servicios esenciales y de operadores de servicios esenciales.*

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

   La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

2. Se identificará a un operador como operador de servicios esenciales si un incidente pudiera tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes criterios:

   a) En relación con la importancia del servicio prestado:

      1º) la disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial;

      2º) la valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la

dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública;

b) En relación con los clientes de la entidad evaluada:

1º) el número de usuarios que confían en los servicios prestados por ella;

2º) su cuota de mercado.

Reglamentariamente, podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.

3. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.

4. En la identificación de los servicios esenciales y de los operadores de servicios esenciales se tendrán en consideración, en la mayor medida posible, las recomendaciones pertinentes que adopte el grupo de cooperación.

5. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará al punto de contacto único de dichos Estados sobre la intención de identificarlo como operador de servicios esenciales.

Artículo 7. *Comunicación de actividad por los proveedores de servicios digitales.*

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

TÍTULO III

Marco estratégico e institucional

Artículo 8. *Marco estratégico de seguridad de las redes y sistemas de información.*

La Estrategia Ciberseguridad Nacional seguirá desarrollando las prioridades, los objetivos estratégicos y las medidas políticas y normativas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, todo ello en el marco y en línea con la Estrategia de Seguridad Nacional.

Para ello, el Consejo de Seguridad Nacional promoverá e impulsará la Estrategia de Ciberseguridad Nacional, de conformidad con lo dispuesto en el artículo 21.1 e) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 9. *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1º) En el caso de que éstos sean, además, operadores críticos designados conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

2º) En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.

b) Para los proveedores de servicios digitales: la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, del Ministerio de Energía, Turismo y Agenda Digital.

c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de régimen Jurídico del sector público: el Ministerio de la Presidencia y para las Administraciones Territoriales, a través del Centro Criptológico Nacional.

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

Artículo 10. *Funciones de las autoridades competentes.*

Las autoridades competentes ejercerán las siguientes funciones:

a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.

b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.

c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.

d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de esta ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.

e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de esta ley, conforme a lo establecido en el artículo 27.

f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 25.

g) Cooperar, en el ámbito de aplicación de esta ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad

ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes conforme a lo establecido en los artículos 14 y 29.

h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 15 y 18.

i) Ejercer la potestad sancionadora en los casos previstos en la presente ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 16.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 24.

Artículo 11. *Equipos de respuesta a incidentes de seguridad informática de referencia.*

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

   a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

      1º) El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

      2º) El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España**,** al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

      El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

      3º) El ESPDEF-CERT, del Mando Conjunto de Ciberdefensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen

   b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

   En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

   Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

Artículo 12. *Requisitos y funciones de los CSIRT de referencia.*

1. Los CSIRT deberán reunir las siguientes condiciones:

   a) Garantizarán un elevado nivel de disponibilidad de sus servicios de comunicaciones evitando los fallos ocasionales y contarán con varios medios para que se les pueda contactar y puedan contactar a otros en todo momento. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos de los grupos de usuarios y los socios colaboradores.

   b) Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros.

   c) Garantizarán la continuidad de las actividades. Para ello:

      1º) Estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.

      2º) Contarán con personal suficiente para garantizar su disponibilidad en todo momento.

      3º) Tener acceso a infraestructuras de comunicación cuya continuidad esté asegurada. A tal fin, se dispondrá de sistemas redundantes y espacios de trabajo de reserva.

   d) Podrán participar, cuando lo deseen, en redes de cooperación internacional.

2. Los CSIRT desempeñarán como mínimo, las siguientes funciones:

   a) Supervisar incidentes a escala nacional.

   b) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados.

   c) Responder a incidentes.

d) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

e) Participar en la red de CSIRT.

3. Los CSIRT establecerán relaciones de cooperación con el sector privado. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas de:

a) Procedimientos de gestión de incidentes y riesgos.

b) Sistemas de clasificación de incidentes, riesgos e información.

Artículo 13. *Punto de contacto único.*

El Consejo de Seguridad Nacional ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9 con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Artículo 14. *Cooperación con otras autoridades con competencias en seguridad de la información, y con las autoridades sectoriales.*

1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.

2. Consultarán asimismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de esta ley, y colaborarán con ellos en el ejercicio de sus funciones.

3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole, al tiempo, cuanta información posean en relación a ello.

TÍTULO IV

Obligaciones de seguridad

Artículo 15. *Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a esta ley.

Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.

2. El desarrollo reglamentario de esta ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer mediante orden ministerial obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

   Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

3. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

4. Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos:

   a) la seguridad de los sistemas e instalaciones;

   b) la gestión de incidentes;

   c) la gestión de la continuidad de las actividades;

   d) la supervisión, auditorías y pruebas;

   e) el cumplimiento de las normas internacionales.

   Los proveedores de servicios digitales atenderán igualmente a los actos de ejecución por los que la Comisión europea detalle los elementos citados.

Artículo 16. *Normas técnicas.*

Las autoridades competentes promoverán la utilización de regulaciones, normas o especificaciones técnicas en materia de seguridad de las redes y sistemas de información elaboradas en el marco del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea.

En ausencia de dichas normas o especificaciones, promoverán la aplicación de las normas o recomendaciones internacionales aprobadas por los organismos internacionales de normalización, y, en su caso, de normas y especificaciones técnicas aceptadas a nivel europeo o internacional que sean pertinentes en esta materia.

Artículo 17. *Sectores con normativa específica equivalente.*

Cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en esta ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

Ello no afectará al deber de cooperación entre autoridades competentes, a la coordinación ejercida por el Consejo de Seguridad Nacional ni, en la medida en que no sea incompatible con la legislación sectorial, a la aplicación del título V sobre notificación de incidentes.

TÍTULO V

Notificación de incidentes

Artículo 18. *Obligación de notificar.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos significativos en dichos servicios.

   Las notificaciones podrán referirse también a los sucesos o incidencias que puedan afectar las redes y sistemas de información empleados para la prestación de los servicios, pero que aún no hayan tenido un efecto adverso real sobre aquellos.

2. Las notificaciones se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos, incluso si éstos son proveedores de servicios digitales sometidos a esta ley.

3. Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

4. El desarrollo reglamentario de esta ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer mediante orden ministerial obligaciones específicas de notificación por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de notificación de incidentes a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

Se aplicará lo dispuesto en el artículo 15.3 a la aplicación de este título y sus disposiciones de desarrollo.

5. La obligación de notificación de incidentes prevista en los apartados anteriores, no obsta al cumplimiento de los deberes legales de denuncia de aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal, y teniendo en cuenta lo previsto en el artículo 14.3 de esta ley.

Artículo 19. *Protección del notificante.*

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.
2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participe en la prestación de los servicios esenciales o digitales que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

   Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

Artículo 20. *Factores y criterios para determinar la importancia de los efectos de un incidente.*

A los efectos de las notificaciones a las que se refiere el artículo 18.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.
c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
f) Importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial
g) El daño reputacional.

Artículo 21. *Notificación inicial, notificaciones intermedias y notificación final.*

1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 18.1 sin dilación indebida.

   La notificación incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.

2. Los operadores de servicios esenciales efectuarán las notificaciones intermedias que sean precisas para actualizar la información incorporada a la notificación inicial e informar sobre la evolución del incidente, mientras éste no esté resuelto.

3. Los operadores de servicios esenciales enviarán una notificación final del incidente tras su resolución.

   Un incidente se considerará resuelto cuando se hayan restablecido las redes y sistemas de información afectados y el servicio opere con normalidad.

4. Lo dispuesto en este artículo se aplicará a las notificaciones de incidentes que padezcan los proveedores de servicios digitales sometidos a esta ley en defecto de lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016.

Artículo 22. *Flexibilidad en la observancia de los plazos para la notificación.*

Los operadores de servicios esenciales y los proveedores de servicios digitales podrán omitir en las comunicaciones que realicen sobre los incidentes que les afecten la información relativa a su repercusión sobre servicios esenciales u otros servicios que dependan de ellos para su prestación, u otra información de la que no dispongan. Tan pronto como conozcan dicha información deberán remitirla a la autoridad competente.

Si, transcurrido un tiempo prudencial desde la notificación inicial del incidente, el operador de servicios esenciales o el proveedor de servicios digitales no ha podido reunir la información pertinente, enviará sin demora un informe justificativo de las actuaciones realizadas para reunir la información y de los motivos por los que no ha sido posible obtenerla, a la autoridad competente.

Artículo 23. *Incidentes que afecten a servicios digitales.*

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a esta ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que está establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.

Artículo 24. *Tramitación de incidentes con impacto transfronterizo.*

1. Cuando las autoridades competentes o los CSIRT de referencia tengan noticia de incidentes que pueden afectar a otros Estados miembros de la Unión Europea, informarán a través del punto de contacto único a los Estados miembros afectados, precisando si el incidente puede tener efectos significativos para los servicios esenciales prestados en dichos Estados.
2. Cuando a través de dicho punto de contacto se reciba información sobre incidentes notificados en otros países de la Unión Europea que puedan tener efectos significativos para los servicios esenciales prestados en España, se remitirá la información relevante a la autoridad competente y al CSIRT de referencia, para que adopten las medidas pertinentes en el ejercicio de sus funciones respectivas.
3. Las actuaciones consideradas en los apartados anteriores se entienden sin perjuicio de los intercambios de información que las autoridades competentes o los CSIRT de referencia puedan realizar de modo directo con sus homólogos de otros Estados miembros de la Unión Europea en relación con aquellos incidentes que puedan resultar de interés mutuo.

Artículo 25. *Información al público.*

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o los proveedores de servicios digitales que informen al público sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en interés público.
2. La autoridad competente también podrá decidir informar de modo directo al público sobre el incidente.

   En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.

Artículo 26. *Confidencialidad de la información sensible.*

Sin perjuicio de lo dispuesto en el artículo 5, al informar sobre incidentes a otras autoridades competentes, a los CSIRT, a otros Estados miembros afectados o al público en general, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales así como la confidencialidad de la información proporcionada en sus notificaciones.

Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

Artículo 27. *Información anual al punto de contacto único y al grupo de cooperación.*

1. Las autoridades competentes transmitirán al punto de contacto único un informe anual sobre el número y tipo de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea.

   Las autoridades competentes elaborarán el informe siguiendo las instrucciones que dicte el punto de contacto único teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

2. El punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año, un informe anual resumido sobre las notificaciones recibidas.

Artículo 28. *Obligación de resolver los incidentes, de información y de colaboración mutua.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.

   En tales casos deberán atender a las indicaciones que reciban del CSIRT para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales han de suministrar al CSIRT de referencia y a la autoridad competente toda la información que se les requiera para el desempeño de sus funciones.

   En particular, podrá requerirse información adicional a los operadores de servicios esenciales y a los proveedores de servicios digitales para analizar la naturaleza, causas y efectos de los incidentes notificados, y para elaborar estadísticas y reunir los datos necesarios para elaborar los informes anuales considerados en el artículo 27.

   Cuando las circunstancias lo permitan, la autoridad competente o el CSIRT proporcionarán a los operadores de servicios esenciales o a los proveedores de servicios digitales afectados por incidentes la información derivada de su seguimiento que pueda serles relevante, en particular, para resolver el incidente.

Artículo 29. *Cooperación en lo relativo a los incidentes que afecten a datos personales.*

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.

Artículo 30. *Autorización para la cesión de datos personales.*

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

Los datos personales intercambiados se cancelarán cuando dejen de ser necesarios para la finalidad que motivó su cesión y, en todo caso, tras la notificación de cierre del incidente. Con posterioridad, los datos personales serán anonimizados.

Artículo 31. *Notificaciones voluntarias.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales podrán notificar los incidentes para los que no se establezca una obligación de notificación.

   Asimismo, las entidades que no hayan sido identificadas como operadores de servicios esenciales y que no sean proveedores de servicios digitales podrán notificar los incidentes que afecten a dichos servicios.

   Estas notificaciones obligan a la entidad que las efectúe a resolver el incidente de acuerdo con lo establecido en el artículo 28.

2. Las notificaciones a las que se refiere el apartado anterior se regirán por lo dispuesto en este título, y se informará sobre ellas al punto de contacto único en el informe anual previsto en el artículo 27.1.

3. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los CSIRT y las autoridades competentes.

TÍTULO VI

Supervisión

Artículo 32. *Supervisión de los operadores de servicios esenciales.*

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

   Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá ordenar al operador que subsane los incumplimientos detectados e indicarle cómo debe hacerlo.

Artículo 33. S*upervisión de los proveedores de servicios digitales.*

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de esta ley cuando tenga noticia de algún incumplimiento por petición razonada de otros órganos o denuncia.

   En tal caso, la autoridad competente podrá requerirle para que le proporcione toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane los incumplimientos detectados.

2. Cuando la autoridad competente tenga noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos por proveedores establecidos en España en otros Estados miembros, adoptará las medias de supervisión pertinentes.

   A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

Artículo 34. *Cooperación transfronteriza.*

1. La supervisión se llevará a cabo, cuando proceda, en cooperación con las autoridades competentes de los Estados miembros en los que se ubiquen las redes y sistemas de información empleados para la prestación del servicio o en que esté establecido el operador de servicios esenciales, el proveedor de servicios digitales o su representante.

2. Las autoridades competentes colaborarán con las autoridades competentes de otros Estados miembros cuando éstas requieran su cooperación en la supervisión y adopción de medidas por operadores de servicios esenciales y proveedores de servicios digitales en relación con las redes y sistemas de información ubicados en España, así como respecto a los proveedores de servicios digitales establecidos en España o cuyo representante en la Unión tenga su residencia o domicilio social en España.

TÍTULO VII

Régimen sancionador

Artículo 35. *Responsables.*

Serán responsables los operadores de servicios esenciales y los proveedores de servicios digitales comprendidos en el ámbito de aplicación de esta ley.

Artículo 36. *Infracciones.*

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.
2. Son infracciones muy graves:
   a) La falta de adopción de medidas para subsanar los incumplimientos detectados, de acuerdo con lo dispuesto en los artículos 32.2 y 33.1, respectivamente, cuando éstos le hayan hecho vulnerable a un incidente con efectos significativos en el servicio y el operador de servicios esenciales o el proveedor de servicios digitales no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.
   b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos significativos en el servicio. Se considerará que es reiterado a partir del segundo incumplimiento.
   c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un impacto significativo en servicios esenciales o servicios digitales en España o en otros Estados miembros.
3. Son infracciones graves:
   a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente referidas a las precauciones mínimas que los operadores de servicios esenciales han de adoptar para garantizar la seguridad de las redes y sistemas de información.
   b) La falta de adopción de medidas para subsanar los incumplimientos detectados en respuesta a un requerimiento dictado de acuerdo con los artículos 32.2 y 33.1 respectivamente, cuando ese sea el tercer requerimiento desatendido que se dicta en los cinco últimos años.
   c) El incumplimiento de la obligación de notificar incidentes con efectos significativos en el servicio.
   d) La demostración de una notoria falta de interés en la resolución de incidentes con impacto significativo notificados cuando dé lugar a una mayor degradación del servicio.

e) Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.

4. Son infracciones leves:

   a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente al amparo de esta ley, cuando no suponga una infracción grave.

   b) La falta de adopción de medidas para corregir los incumplimientos detectados en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 y 33.1, respectivamente.

   c) No facilitar la información que sea requerida por las autoridades competentes sobre sus políticas de seguridad, o proporcionar información incompleta o tardía sin justificación.

   d) No someterse a una auditoría de seguridad o poner obstáculos a la realizada por la Administración, según lo ordenado por la autoridad competente.

   e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten en virtud del artículo 28.2.

   f) La falta de notificación de incidentes sin impacto significativo en el servicio en los casos en que las disposiciones reglamentarias de desarrollo de esta ley obliguen a notificarlos.

   g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 22, o no remitir el informe justificativo sobre la imposibilidad de reunir la información previsto en dicho artículo.

   h) No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente, de acuerdo con el artículo 28.

Artículo 37. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones de multa:

   a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.

   b) Por la comisión de infracciones graves, muta de 100.001 hasta 500.000 euros.

   c) Por la comisión de infracciones leves, amonestación o multa hasta 100.000 euros.

2. Las infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el "Boletín Oficial del Estado" y en el sitio de internet de la autoridad competente, en atención a los hechos concurrentes y de conformidad con el artículo siguiente.

Artículo 38. *Graduación de la cuantía de las sanciones.*

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

e) El número de usuarios afectados.

f) El volumen de facturación del responsable.

g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.

h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

Artículo 39. *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 38.
   b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
   c) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
   d) 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.

3. No podrán ser objeto de apercibimiento las infracciones leves descritas en el artículo 36.4 c), d) y e) y la infracción grave prevista en el artículo 36.3 e).

Artículo 40. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 36 fuesen cometidas por órganos o entidades de las Administraciones Públicas, 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 órgano o entidad infractora y a los afectados, si los hubiera.

Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.

2. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refiere el apartado anterior.

Artículo 41. *Competencia sancionadora.*

1. La imposición de sanciones corresponderá, en el caso de infracciones muy graves, al Ministro competente en virtud de lo dispuesto en el artículo 9, y en el caso de infracciones graves y leves al órgano de la autoridad competente que se determine mediante el reglamento de desarrollo de esta ley.

2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previsto en las Leyes 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas, y 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Artículo 42. *Concurrencia de infracciones.*

1. 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.

2. 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.

Disposición adicional primera. *Relación inicial de servicios esenciales y operadores de servicios esenciales*

La Comisión Nacional para la Protección de las Infraestructuras Críticas aprobará una primera lista de servicios esenciales dentro de los sectores incluidos en el ámbito de aplicación de esta ley e identificará a los operadores que los presten que deban sujetarse a esta ley en el siguiente orden:

a) Antes del 9 de noviembre de 2018: los servicios esenciales y los operadores correspondientes a los sectores estratégicos energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

b) Antes del 9 de noviembre de 2019: los servicios esenciales y los operadores correspondientes al resto de los sectores estratégicos recogidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Disposición adicional segunda. *Comunicaciones electrónicas y servicios de confianza.*

La aplicación de esta ley a los operadores de redes y servicios de comunicaciones electrónicas y de servicios electrónicos de confianza que sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, no obstará a la aplicación de su normativa específica en materia de seguridad.

El Ministerio de Energía, Turismo y Agenda Digital, como órgano competente para la aplicación de dicha normativa, y el Ministerio del Interior actuarán de manera coordinada en el establecimiento de obligaciones que recaigan sobre los operadores críticos. Así mismo, mantendrán un intercambio fluido de información sobre incidentes que les afecten.

Disposición adicional tercera. *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en esta ley.*

La plataforma común para la notificación de incidentes prevista en esta ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el 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, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

Disposición transitoria única. *Proveedores de servicios digitales ya existentes.*

Los proveedores de servicios digitales que ya vinieran prestando servicios deberán comunicar su actividad al Ministerio de Energía, Turismo y Agenda Digital en el plazo de tres meses desde la entrada en vigor de esta ley.

Disposición final primera. *Fundamento constitucional.*

Esta ley se dicta en virtud de las competencias atribuidas al Estado por el artículo 149.1.21ª y 29ª de la Constitución.

Disposición final segunda. *Incorporación del Derecho de la Unión Europea.*

Esta ley incorpora al Ordenamiento jurídico interno la 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.

Disposición final tercera. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno para desarrollar mediante real decreto lo previsto en esta ley.