NORMATIVAS DE CIBERSEGURIDAD

Unidad 3. Actividad 2

22 DE ENERO DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado....2
RESUMEN DEL Real Decreto-ley 12/2018....2
TÍTULO I....2
Disposiciones generales....2
TÍTULO II....4
Servicios esenciales y servicios digitales....4
TÍTULO IV....8
Obligaciones de seguridad....8
TÍTULO V....9
Notificación de incidentes....9
TÍTULO VI....12
Supervisión....12
TÍTULO VII....13
Régimen sancionador....13

Enunciado

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.-

RESUMEN DEL Real Decreto-ley 12/2018

TÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. El presente real decreto-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 este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Artículo 2. Ámbito de aplicación. 1. Este real decreto-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.

B Los servicios digitales, considerados conforme se determina en el artículo.

2. Estarán sometidos a este real decreto-ley:

a) Los operadores de servicios esenciales establecidos en España.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea.

3. Este real decreto-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.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas.

Artículo 3. Definiciones.

A los efectos de este real decreto-ley, se entenderá por:

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

1.º Las redes de comunicaciones electrónicas.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º 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.

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas.

d) Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a)

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.

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 éste.

j) Representante: persona física o jurídica establecida en la Unión Europea que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea

k) Norma técnica

l) Especificación: una especificación técnica en el sentido del artículo 2.4

m) Punto de intercambio de Internet: una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet.

n) Sistema de nombres de dominio

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

p) Registro de nombres de dominio 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.

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

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 este real decreto-ley y en la elaboración de los reglamentos y guías previstos en él 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.

Artículo 5. Salvaguarda de funciones estatales esenciales.

Lo dispuesto en este real decreto-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.

TÍTULO II

Servicios esenciales y servicios digitales

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.

a) En relación con la importancia del servicio prestado:

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial.

2.º 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.

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

1.º El número de usuarios que confían en los servicios prestados por ella

2.º Su cuota de mercado.

2. bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.

3. 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.

4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos 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.

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

La Estrategia de Ciberseguridad Nacional, al amparo y alineada con la Estrategia de Seguridad Nacional, enmarca los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.

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:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

2.º 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 de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos.

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

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 este real decreto-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 este real decreto-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 26.

g) Cooperar, en el ámbito de aplicación de este real decreto-ley,

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 16 y 19.

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-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 17.

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 25.

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.

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.

3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

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.

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

c) Garantizarán la continuidad de las actividades.

d) Deberán tener la capacidad de 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.

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 así mismo, 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 este real decreto-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 con ello.

Artículo 15. Confidencialidad de la información sensible.

TÍTULO IV

Obligaciones de seguridad

Artículo 16. 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 este real decreto-ley.

2. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.

3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información.

4. 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

5. 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.

6. 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.

7. 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.

Artículo 17. 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.

Artículo 18. 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 este real decreto-ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

TÍTULO V

Notificación de incidentes

Artículo 19. Obligación de notificar.

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

2. Así mismo, los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.

3. Las notificaciones tanto de operadores de servicios esenciales como de proveedores de servicios digitales se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados.

4. 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.

5. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales.

6. 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.

Artículo 20. 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, participen en la prestación de los servicios esenciales o digitales

Artículo 21. Factores para determinar la importancia de los efectos de un incidente.

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, 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) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.

g) El daño a la reputación.

2. En las notificaciones a las que se refiere el artículo 19.2, la importancia de un incidente se determinará conforme a lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE).

Artículo 22. 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 19.1 sin dilación indebida.

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.

Artículo 23. 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 de la que aún no dispongan 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.

Artículo 24. Incidentes que afecten a servicios digitales.

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este real decreto-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 estuviese establecido el citado proveedor.

Artículo 25. 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.

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 perturbadores significativos para los servicios esenciales prestados en España.

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 26. Información al público.

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes.

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente.

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.

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, y lo remitirá ulteriormente a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

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

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 las funciones.

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.

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.

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.

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 por 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.

2. A la vista de la información recabada, la autoridad competente podrá requerir al operador que subsane las deficiencias detectadas e indicarle cómo debe hacerlo.

Artículo 33. Supervisión 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 este real decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia.

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

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.

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 este real decreto-ley.

Artículo 36. Infracciones

1. Las infracciones de los preceptos de este real decreto-ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La falta de adopción de medidas para subsanar las deficiencias detectadas

b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un efecto perturbador significativo en la prestación servicios esenciales o de 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 las deficiencias detectadas en respuesta a un requerimiento dictado.

c) El incumplimiento de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

d) La demostración de una notoria falta de interés en la resolución de incidentes con efectos perturbadores significativos 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.

f) Poner obstáculos a la realización de auditorías por la autoridad competente.

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 este real decreto-ley, cuando no suponga una infracción grave.

b) La falta de adopción de medidas para corregir las deficiencias detectadas en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 o 33.1.

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 según lo ordenado por la autoridad competente.

e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten.

f) La falta de notificación de los sucesos o incidencias para los que, aunque no hayan tenido un efecto adverso real sobre los servicios, exista obligación de notificación en virtud del párrafo segundo del artículo 19.2.

g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 23, 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

Artículo 37. Sanciones

1. Por la comisión de las infracciones recogidas en el artículo anterior.

2. Las sanciones firmes en vía administrativa por 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 último 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. Proporcionalidad de sanciones.

1. El órgano sancionador podrá establecer 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 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.

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 no acordar el inicio del procedimiento sancionador

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en este real decreto-ley.

b) Que el órgano competente no hubiese sancionado o apercibido al infractor en los dos años previos como consecuencia de la comisión de infracciones previstas en este real decreto-ley.

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.

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.

2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previstos en las Leyes 39/2015.

3. El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones públicas.

Artículo 42. Concurrencia de infracciones.

1. No procederá la imposición de sanciones según lo previsto en este real decreto-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.