Consejo de la Unión Europea

Bruselas, 21 de abril de 2016
(OR. en)

5581/16

Expediente interinstitucional: 2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

ACTOS LEGISLATIVOS Y OTROS INSTRUMENTOS

Asunto:	Posición del Consejo en primera lectura con vistas a la adopción de una DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

DIRECTIVA (UE) 2016/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de …

relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[1],

De conformidad con el procedimiento legislativo ordinario[2],

[1] DO C 271 de 19.9.2013, p. 133.

[2] Posición del Parlamento Europeo de 13 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y Posición del Consejo en primera lectura de … (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de … (pendiente de publicación en el Diario Oficial).

Considerando lo siguiente:

(1) Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior.

(2) La magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información. Esos sistemas pueden convertirse además en objetivo de acciones nocivas deliberadas destinadas a perjudicar o interrumpir su funcionamiento. Este tipo de incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, menoscabar la confianza del usuario y causar grandes daños a la economía de la Unión.

(3) Las redes y sistemas de información, principalmente Internet, contribuyen de forma decisiva a facilitar la circulación transfronteriza de bienes, servicios y personas. Debido a ese carácter transnacional, una perturbación grave de esas redes y sistemas, ya sea o no deliberada, y con independencia del lugar en que se produzca, puede afectar a diferentes Estados miembros y a la Unión en su conjunto. Por consiguiente, la seguridad de las redes y sistemas de información es fundamental para el correcto funcionamiento del mercado interior.

(4) Partiendo de los significativos avances logrados en el marco del Foro Europeo de Estados miembros, que ha permitido promover discusiones e intercambios de información sobre buenas prácticas políticas, incluida la elaboración de principios de cooperación europea ante crisis cibernéticas, procede establecer un Grupo de cooperación compuesto por representantes de los Estados miembros, la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) a fin de respaldar y facilitar la cooperación estratégica entre los Estados miembros en lo relativo a la seguridad de las redes y sistemas de información. Para que dicho grupo sea eficaz e integrador, es esencial que todos los Estados miembros posean unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las redes y sistemas de información en su territorio. Por otra parte, los operadores de servicios esenciales y los proveedores de servicios digitales deben estar sujetos a requisitos en materia de seguridad y notificación de incidentes, con el fin de fomentar una cultura de gestión de riesgos y garantizar que se informe de los incidentes más graves.

(5) Las capacidades existentes no bastan para garantizar un elevado nivel de seguridad de las redes y sistemas de información en la Unión. Los niveles de preparación de los Estados miembros son muy distintos, lo que ha dado lugar a planteamientos fragmentados en la Unión. Esta situación genera niveles desiguales de protección de los consumidores y las empresas, comprometiendo el nivel general de seguridad de las redes y sistemas de información de la Unión. A su vez, la inexistencia de requisitos comunes aplicables a los operadores de servicios esenciales y los proveedores de servicios digitales imposibilita la creación de un mecanismo global y eficaz de cooperación en la Unión. Las universidades y los centros de investigación tienen un papel determinante que desempeñar a la hora de impulsar la investigación, el desarrollo y la innovación en esos ámbitos.

(6) Para dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información es necesario un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales. No obstante, no está excluido que los operadores de servicios esenciales y los proveedores de servicios digitales apliquen medidas de seguridad más estrictas que las previstas en la presente Directiva.

(7) Para cubrir todos los incidentes y riesgos pertinentes, la presente Directiva debe aplicarse tanto a los operadores de servicios esenciales como a los proveedores de servicios digitales. Sin embargo, las obligaciones impuestas a los operadores de servicios esenciales y a los proveedores de servicios digitales no deben aplicarse a empresas que suministren redes públicas de comunicaciones o presten servicios de comunicaciones electrónicas disponibles para el público en el sentido de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo[1], que están sujetas a los requisitos específicos de seguridad e integridad establecidos en dicha Directiva, como tampoco a los prestadores de servicios de confianza definidos en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo[2], que están sujetos a los requisitos de seguridad establecidos en dicho Reglamento.

---

1 Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) (DO L 108 de 24.4.2002, p. 33).

2 Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

(8) La presente Directiva debe entenderse sin perjuicio de que los Estados miembros puedan adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de su seguridad, preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales. De conformidad con el artículo 346 del Tratado de Funcionamiento de la Unión Europea (TFUE), ningún Estado miembro está obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad. En este contexto, son relevantes la Decisión del Consejo 2013/488/UE[1] y los acuerdos sobre confidencialidad o los acuerdos informales sobre confidencialidad como el Protocolo para el intercambio de información.

(9) Determinados sectores de la economía ya están ya regulados o pueden regularse en el futuro mediante actos jurídicos sectoriales de la Unión que incluyan normas relacionadas con la seguridad de las redes y sistemas de información. Siempre que esos actos jurídicos de la Unión contengan disposiciones por las que se impongan requisitos en materia de seguridad de las redes y sistemas de información o en materia de notificación de incidentes, dichas disposiciones deben aplicarse en lugar de las disposiciones correspondientes de la presente Directiva si contienen requisitos cuyos efectos sean, como mínimo, equivalentes a los de las obligaciones que establece la presente Directiva. En tales casos, los Estados miembros deben aplicar lo dispuesto en los mencionados actos jurídicos sectoriales de la Unión, incluidos los relativos a cuestiones de competencia judicial, y no deben llevar a cabo el proceso de identificación de los operadores de servicios esenciales, tal como se definen en la presente Directiva. En este contexto, los Estados miembros deben facilitar a la Comisión información sobre la aplicación de dichas disposiciones con carácter de *lex specialis*. A la hora de determinar si los requisitos en materia de seguridad de las redes y sistemas de información o en materia de notificación de incidentes establecidos en los actos jurídicos sectoriales de la Unión son o no equivalentes a los que se establecen en la presente Directiva, debe tenerse únicamente en cuenta lo dispuesto en los actos jurídicos de la Unión aplicables y su aplicación en los Estados miembros.

[1] Decisión 2013/488/UE del Consejo, de 23 de septiembre de 2013, sobre las normas de seguridad para la protección de la información clasificada de la UE (DO L 274 de 15.10.2013, p. 1).

(10) En el sector del transporte marítimo y fluvial, los requisitos de seguridad que imponen los actos jurídicos de la Unión a las compañías, buques, instalaciones portuarias, puertos y servicios de gestión del tráfico de buques se aplican a la totalidad de las operaciones, incluidas las de los sistemas de radio y telecomunicaciones, los sistemas informáticos y las redes. Una parte de los procedimientos obligatorios que han de seguirse se refiere a la notificación de todos los incidentes de seguridad, y debe, por tanto, considerarse *lex specialis* en la medida en que dichos requisitos sean al menos equivalentes a las disposiciones correspondientes de la presente Directiva.

(11) Al identificar a los operadores del sector del transporte marítimo y fluvial, los Estados miembros deben tener en cuenta los códigos y directrices internacionales existentes o que se puedan elaborar en el futuro, en particular, por parte de la Organización Marítima Internacional, con el fin de proporcionar a los diferentes operadores marítimos un planteamiento coherente.

(12) La regulación y la supervisión del sector bancario y de las infraestructuras de los mercados financieros han sido objeto de una elevada armonización en la Unión mediante el recurso al Derecho primario y al Derecho derivado de la Unión y a normas elaboradas junto con las Autoridades Europeas de Supervisión. Dentro de la Unión Bancaria, el Mecanismo Único de Supervisión garantiza la aplicación y supervisión de dichos requisitos. En los Estados miembros que no forman parte de la Unión Bancaria, son los reguladores bancarios competentes de cada Estado miembro los que garantizan dicha función. En otros ámbitos de regulación del sector financiero, el Sistema Europeo de Supervisión Financiera también garantiza un alto grado de uniformidad y convergencia de las prácticas de supervisión. La Autoridad Europea de Valores y Mercados también desempeña una función directa de supervisión para determinadas entidades, concretamente las agencias de calificación crediticia y los registros de operaciones.

(13) El riesgo operativo es un componente fundamental de la regulación y la supervisión prudenciales en los sectores de la banca y las infraestructuras del mercado financiero. Dicho riesgo se extiende a todas las operaciones, incluidas la seguridad, la integridad y la resistencia de las redes y sistemas de información. Los requisitos relativos a estos sistemas, que a menudo son más estrictos que los establecidos en la presente Directiva, se recogen en una serie de actos jurídicos de la Unión que incluyen normas sobre el acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, y normas sobre los requisitos prudenciales aplicables a las entidades de crédito y las empresas de inversión, que incluyen requisitos sobre el riesgo operativo; normas sobre los mercados de instrumentos financieros, que incluyen requisitos sobre evaluación de riesgos para las empresas de inversión y los mercados regulados; normas sobre los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones, que incluyen requisitos sobre el riesgo operativo para dichas entidades y registros; y normas sobre la mejora de la liquidación de valores en la Unión y sobre los depositarios centrales de valores, que incluyen requisitos sobre el riesgo operativo. Por otra parte, los requisitos de notificación de incidentes forman parte de la práctica normal en materia de supervisión en el sector financiero y están incluidos a menudo en los manuales de supervisión. Los Estados miembros deben tener en cuenta dichas normas y requisitos a la hora de aplicar la *lex specialis*.

(14) Como ya observó el Banco Central Europeo en su dictamen de 25 de julio de 2014[1], la presente Directiva no afecta al régimen de supervisión de los sistemas de pago y liquidación del Eurosistema en virtud del Derecho de la Unión. Conviene que las autoridades responsables de esa supervisión intercambien experiencias sobre cuestiones relacionadas con la seguridad de las redes y sistemas de información con las autoridades competentes en virtud de la presente Directiva. Esta consideración se aplica asimismo a los miembros del Sistema Europeo de Bancos Centrales que no sean miembros de la zona Euro y que ejerzan esa supervisión de los sistemas de pago y liquidación sobre la base de disposiciones legales y reglamentarias nacionales.

[1] DO C 352 de 7.10.2014, p. 4.

(15) Los mercados en línea permiten a consumidores y comerciantes celebrar contratos de compraventa o de prestación de servicios en línea con comerciantes, y son el destino final de celebración de tales contratos. Esos mercados no deben tener por objeto servicios en línea que constituyan únicamente un paso intermedio para acceder a servicios prestados por terceros a través de los que finalmente se pueda celebrar un contrato. Por consiguiente, no deben tener por objeto servicios en línea que comparen el precio de los productos o servicios de diferentes comerciantes para luego dirigir al usuario hacia el comerciante al que este prefiera comprar el producto. Los servicios informáticos prestados por el mercado en línea pueden incluir servicios de tramitación de transacciones, agregación de datos o elaboración de perfiles de los usuarios. Las tiendas de aplicaciones, que funcionan como tiendas en línea que posibilitan la distribución digital de aplicaciones o programas informáticos de terceros, deben ser consideradas un tipo de mercado en línea.

(16) Los motores de búsqueda en línea permiten al usuario realizar búsquedas, en principio, en todos los sitios web, a partir de una consulta sobre cualquier tema. También pueden restringirse a sitios web en una lengua determinada. La definición de «motor de búsqueda en línea» de la presente Directiva no debe incluir las funciones de búsqueda que se limiten al contenido de un sitio web en concreto, con independencia de que la función de búsqueda la proporcione un motor de búsqueda externo. Tampoco debe incluir, por consiguiente, servicios en línea que comparen el precio de los distintos productos o servicios de diferentes comerciantes para luego dirigir al usuario hacia el comerciante al que se prefiera comprar el producto.

(17) Los servicios de computación en nube abarcan toda una serie de actividades que pueden realizarse según diferentes modelos. A efectos de la presente Directiva, se entiende por «servicios de computación en nube» aquellos servicios que permiten acceder a un conjunto modulable y elástico de recursos informáticos que se pueden compartir. Esos «servicios de computación» incluyen recursos tales como las redes, servidores u otras infraestructuras, sistemas de almacenamiento, aplicaciones y servicios. El término «modulable» se refiere a los recursos de computación que el proveedor de servicios en nube puede asignar de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término «elástico» se usa para describir los recursos de los que se abastece y que se ponen a la venta según la demanda, de modo que se puedan aumentar o reducir con rapidez los recursos disponibles en función de la carga de trabajo. La expresión «que se pueden compartir» se usa para describir recursos informáticos que se proporcionan a múltiples usuarios que comparten un acceso común al servicio pero la tramitación se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico.

(18) La función de un punto de intercambio de Internet (en lo sucesivo, «IXP», por sus siglas en inglés de «Internet Exchange Point») es conectar redes entre sí. Un IXP no proporciona acceso a la red ni actúa como proveedor o transportista de servicios de tránsito. Tampoco presta otros servicios ajenos a la interconexión, aunque ello no impide que un IXP preste tales servicios. El IXP existe para conectar entre sí redes que están técnica y organizativamente diferenciadas. El término «sistema autónomo» se emplea para describir una red que es técnicamente independiente.

(19) Los Estados miembros deben ser responsables de determinar qué entidades cumplen los criterios de la definición de «operador de servicios esenciales». A efectos de garantizar un planteamiento coherente, la definición de operador de servicios esenciales debe ser aplicada de manera coherente por todos los Estados miembros. A tal fin, la presente Directiva prevé un examen de las entidades que desarrollan su actividad en sectores y subsectores específicos, el establecimiento de una lista de servicios esenciales, la consideración de una lista común de factores intersectoriales que permitan determinar si un incidente potencial tendría un efecto perturbador significativo, un proceso de consulta en el que participen los Estados miembros pertinentes en el caso de las entidades que prestan servicios en varios Estados miembros, y el apoyo del Grupo de cooperación en el proceso de identificación. Con el fin de garantizar que los cambios que puedan producirse en el mercado se tengan debidamente en cuenta, los Estados miembros deben revisar periódicamente la lista de operadores identificados y actualizarla cuando sea necesario. Por último, los Estados miembros deben presentar a la Comisión la información necesaria para valorar en qué medida este método común ha permitido que los Estados miembros apliquen la definición de modo coherente.

(20) En el proceso de identificación de los operadores de servicios esenciales, los Estados miembros deben valorar, como mínimo para cada uno de los subsectores que se indican en la presente Directiva, qué servicios han de considerarse esenciales para el mantenimiento de actividades sociales y económicas vitales y determinar si las entidades enumeradas en los sectores y subsectores que se indican en la presente Directiva y que prestan esos servicios cumplen los criterios de identificación de los operadores. Al valorar si una entidad presta un servicio que es esencial para el mantenimiento de actividades sociales o económicas cruciales, basta con examinar si la entidad presta un servicio que esté incluido en la lista de servicios esenciales. Por otra parte, debe demostrarse que la prestación del servicio esencial depende de redes y sistemas de información. Por último, al valorar si un incidente en las redes y sistemas de información relativo a la prestación del servicio tendría un efecto perturbador significativo en la prestación de este, los Estados miembros deben tener en cuenta una serie de factores intersectoriales, así como, en su caso, los factores sectoriales pertinentes.

(21) A efectos de la identificación de los operadores de servicios esenciales, el establecimiento en un Estado miembro implica el ejercicio real y efectivo de una actividad mediante una organización estable. La forma jurídica de dicha organización, ya sea a través de una sucursal o una filial con personalidad jurídica, no es el factor determinante a este respecto.

(22) Es posible que las entidades que operan en los sectores y subsectores que se indican en la presente Directiva presten tanto servicios esenciales como no esenciales. Por ejemplo, en el sector del transporte aéreo, los aeropuertos prestan servicios que un Estado miembro puede considerar esenciales, como la gestión de las pistas, pero también una serie de servicios que pueden considerarse no esenciales, como la oferta de zonas comerciales. Los operadores de servicios esenciales deben estar sujetos a los requisitos específicos de seguridad únicamente respecto de aquellos servicios que se consideren esenciales. Para la identificación de los operadores, los Estados miembros deben por lo tanto establecer una lista de los servicios que se consideren esenciales.

(23) La lista de servicios debe contener la totalidad de los servicios prestados en el territorio de un determinado Estado miembro que cumplan los requisitos establecidos en la presente Directiva. Los Estados miembros deben estar facultados para completar la lista existente incluyendo en ella nuevos servicios. La lista de servicios debe servir de referencia para que los Estados miembros puedan identificar a los operadores de servicios esenciales. Su finalidad es determinar los tipos de servicios esenciales en cada uno de los sectores que se indican en la presente Directiva, distinguiéndolos así de los servicios no esenciales de los que una entidad activa en un sector determinado pueda ser responsable. La lista de servicios establecida por cada Estado miembro sería otro elemento de utilidad para evaluar las prácticas normativas de cada Estado miembro con el fin de garantizar la coherencia global del proceso de identificación en todos los Estados miembros.

(24) Para los fines del proceso de identificación, cuando una entidad preste un servicio esencial en dos o más Estados miembros, estos deben entablar entre sí conversaciones bilaterales o multilaterales. Este proceso de consulta tiene por objeto ayudarles a valorar el carácter critico del operador en términos de su impacto transfronterizo, permitiendo a cada Estado miembro participante exponer su punto de vista en lo que respecta a los riesgos asociados a los servicios prestados. Los Estados miembros interesados deben tener en cuenta los puntos de vista de los demás en este proceso, y deben poder solicitar la asistencia del Grupo de cooperación a este respecto.

(25) Como resultado del proceso de identificación, los Estados miembros deben adoptar medidas nacionales para determinar qué entidades están sujetas a obligaciones en materia de seguridad de las redes y sistemas de información. Este resultado podría alcanzarse mediante la elaboración de una lista en la que se enumere a todos los operadores de servicios esenciales, o bien mediante la adopción de medidas nacionales que incluyan criterios objetivos y cuantificables, como la producción del operador o el número de usuarios, que permitan determinar qué entidades han de quedar sujetas a las obligaciones en materia de seguridad de las redes y sistemas de información. Las medidas nacionales, con independencia de que ya existieran o de que se adopten en el contexto de la presente Directiva, deben incluir todas las medidas jurídicas y administrativas y las políticas que permitan identificar a los operadores de servicios esenciales a los efectos de la presente Directiva.

(26) Para dar una indicación de la importancia, en relación con el sector de que se trate, de los operadores identificados de servicios esenciales, los Estados miembros deben tener en cuenta el número y la magnitud de los operadores identificados, por ejemplo en términos de cuota de mercado o cantidad producida o transportada, sin necesidad de divulgar información que pueda revelar qué operadores han sido identificados.

(27) A fin de determinar si un incidente podría tener un efecto perturbador significativo, los Estados miembros deben tener en cuenta distintos factores, como el número de usuarios que confían en dicho servicio para fines tanto privados como profesionales. La utilización de ese servicio puede ser directa, indirecta o mediante intermediario. Al evaluar el impacto, en términos de magnitud y duración, que podría tener un incidente en las actividades económicas y sociales o en la seguridad pública, los Estados miembros deben considerar también el tiempo que probablemente tendría que transcurrir antes de que la discontinuidad empiece a tener repercusiones negativas.

(28) Además de los factores intersectoriales, deben también tenerse en cuenta factores específicamente sectoriales para determinar si un incidente tendría un efecto perturbador significativo en la prestación de un servicio esencial. En el caso de los proveedores de energía, esos factores podrían ser el volumen o la proporción de la energía nacional generada; en el caso de los proveedores de petróleo, el volumen diario; en el caso del transporte aéreo, incluidos aeropuertos y compañías aéreas, del transporte ferroviario y de los puertos marítimos, la proporción del volumen de tráfico nacional y el número de viajeros u operaciones de transporte de mercancías anuales; en el caso de la banca o las infraestructuras del mercado financiero, su importancia sistémica, valorada según los activos totales o la razón entre estos y el producto interior bruto; en el caso del sector sanitario, el número de pacientes atendidos cada año por el prestador de servicios sanitarios; en el caso de la producción, tratamiento y abastecimiento de agua, el volumen y el número y los tipos de usuarios abastecidos incluidos, por ejemplo, hospitales, organismos que presten servicios públicos o particulares, y la existencia de fuentes alternativas de suministro de agua para abastecer la misma zona geográfica.

(29) A fin de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, cada Estado miembro debe disponer de una estrategia nacional de seguridad de las redes y sistemas de información que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar.

(30) Habida cuenta de las diferencias existentes entre las estructuras nacionales de gobernanza y con el fin de salvaguardar las disposiciones sectoriales vigentes o los organismos de supervisión y regulación de la Unión ya existentes, y para evitar duplicidades, los Estados miembros deben poder designar a más de una autoridad nacional competente responsable de ejercer las funciones vinculadas a la seguridad de las redes y sistemas de información de los operadores de servicios esenciales y los proveedores de servicios digitales en virtud de la presente Directiva.

(31) Con el fin de facilitar la cooperación y la comunicación transfronterizas y de permitir una aplicación efectiva de la presente Directiva, es necesario que cada Estado miembro designe, sin perjuicio de las disposiciones normativas sectoriales, un punto de contacto único nacional que se encargue de coordinar las cuestiones relacionadas con la seguridad de las redes y sistemas de información y de la cooperación transfronteriza a escala de la Unión. Las autoridades competentes y los puntos de contacto único deben disponer de recursos técnicos, financieros y humanos adecuados para garantizar que puedan ejercer de manera efectiva y eficiente las funciones que se les atribuyen y alcanzar de este modo los objetivos de la presente Directiva. Dado que la finalidad de la presente Directiva es mejorar el funcionamiento del mercado interior mediante la creación de un clima de confianza y seguridad, los organismos de los Estados miembros deben poder cooperar eficazmente con los agentes económicos y han de estar estructurados en consecuencia.

(32) Las autoridades competentes o los equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «CSIRT», por sus siglas en inglés de «Computer Security Incident Response Teams») deben recibir las notificaciones de los incidentes. Los puntos de contacto únicos no deben recibir directamente ninguna notificación de incidente, salvo en caso de que actúen también como autoridad competente o como CSIRT. No obstante, una autoridad competente o un CSIRT ha de poder encargar al punto de contacto único que transmita notificaciones de incidentes a los puntos de contacto únicos de los demás Estados miembros afectados.

(33) Para garantizar que la información se facilite efectivamente a los Estados miembros y a la Comisión, el punto de contacto único debe presentar un informe resumido al Grupo de cooperación, y este debe estar anonimizado para proteger la confidencialidad de las notificaciones y la identidad de los operadores de servicios esenciales y los proveedores de servicios digitales, dado que, para el intercambio de información sobre buenas prácticas dentro del Grupo de cooperación, no es necesaria información sobre la identidad de las entidades notificantes. El informe resumido debe contener información sobre el número de notificaciones recibidas y sobre las características de los incidentes notificados, como los tipos de vulneraciones de la seguridad, su gravedad o su duración.

(34) Los Estados miembros deben disponer de capacidades técnicas y de organización adecuadas para poder adoptar medidas de prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las redes y sistemas de información. Los Estados miembros deben asegurarse por tanto de que disponen de CSIRT que funcionen adecuadamente y cumplan los requisitos esenciales para así disponer de capacidades efectivas y compatibles que permitan hacer frente a incidentes y riesgos y garantizar una cooperación eficaz a escala de la Unión. Con el fin de que todos los tipos de operadores de servicios esenciales y proveedores de servicios digitales gocen de este tipo de capacidades y posibilidades de cooperación, los Estados miembros deben asegurarse de que todos ellos queden cubiertos por un CSIRT designado. Dada la importancia de la cooperación internacional en materia de ciberseguridad, los CSIRT deben tener la posibilidad de participar en redes internacionales de cooperación además de la red de CSIRT establecida en virtud de la presente Directiva.

(35) La cooperación entre los sectores público y privado es esencial dado que la mayor parte de las redes y sistemas de información es de gestión privada. Se debe alentar a los operadores de servicios esenciales y proveedores de servicios digitales a crear sus propios mecanismos de cooperación informal para garantizar la seguridad de las redes y sistemas de información. Cuando sea indicado, el Grupo de cooperación ha de poder invitar a los interesados a las discusiones. Para fomentar eficazmente el intercambio de información y buenas prácticas, es esencial garantizar que los operadores de servicios esenciales y los proveedores de servicios digitales que participan en dichos intercambios no queden en desventaja a causa de su cooperación.

(36) La ENISA debe prestar asistencia a los Estados miembros y a la Comisión ofreciéndoles su experiencia, conocimientos y asesoramiento y facilitando el intercambio de buenas prácticas. En particular, a la hora de aplicar la presente Directiva, la Comisión debe consultar a la ENISA, y los Estados miembros deben poder hacerlo. Para desarrollar las capacidades y los conocimientos en los Estados miembros, el Grupo de cooperación debe servir también de instrumento para intercambiar información sobre buenas prácticas, discutir sobre las capacidades y el grado de preparación de los Estados miembros y, a título voluntario, prestar ayuda a los miembros del grupo para evaluar las estrategias nacionales en materia de seguridad de las redes y sistemas de información, la creación de capacidades y los ejercicios de evaluación relativos a la seguridad de las redes y sistemas de información.

(37) En su caso, los Estados miembros deben poder utilizar o adaptar las estructuras organizativas o las estrategias existentes al aplicar la presente Directiva.

(38) Las funciones del Grupo de cooperación y las de la ENISA son interdependientes y complementarias. En general, la ENISA debe ayudar al Grupo de cooperación en la ejecución de sus funciones, en consonancia con el objetivo de aquella, establecido en el artículo 2 del Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo[1], a saber, ayudar a las instituciones, órganos y organismos de la Unión y a los Estados miembros a aplicar las políticas necesarias para cumplir los requisitos legales y reglamentarios relativos a la seguridad de las redes y de la información que figuran en actos jurídicos actuales y futuros de la Unión. En particular, la ENISA debe prestar asistencia en aquellos ámbitos que corresponden a sus propias funciones, enumeradas el Reglamento (UE) n.º 526/2013, a saber, analizar las estrategias de la seguridad de las redes y los sistemas de información, apoyar la organización y realización de ejercicios relativos a la seguridad de las redes y sistemas de información a escala de la Unión e intercambiar información y buenas prácticas en materia de sensibilización y formación. La ENISA también debe participar en la elaboración de las directrices aplicables a los criterios sectoriales de determinación de la gravedad de las repercusiones de un incidente.

(39) A fin de promover un elevado nivel de seguridad de las redes y sistemas de información, el Grupo de cooperación debe, en su caso, cooperar con las instituciones, órganos y organismos de la Unión para intercambiar conocimientos prácticos y buenas prácticas, y para ofrecer asesoramiento sobre aspectos de seguridad de las redes y sistemas de información que puedan incidir en la labor de dichas instituciones, órganos y organismos, sin dejar de respetar las disposiciones vigentes en materia de intercambio de información restringida. Cuando coopere con las autoridades policiales en los aspectos relacionados con la seguridad de las redes y de la información que puedan incidir en la labor de dichas autoridades, el Grupo de cooperación debe respetar los canales de información existentes y las redes establecidas.

---

[1] Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004 (DO L 165 de 18.6.2013, p. 41).

(40) La información sobre incidentes tiene cada vez mayor utilidad para la población en general y para las empresas, en particular las pequeñas y medianas empresas. En algunos casos, este tipo de información ya se proporciona a través de sitios web de ámbito nacional, en la lengua de un país concreto, dedicados principalmente a incidentes y sucesos con una dimensión nacional. Dado que las empresas operan cada vez más con carácter transfronterizo y que los particulares utilizan servicios en línea, la información sobre incidentes debe facilitarse de modo agregado a escala de la Unión. Es conveniente que la secretaría de la red de CSIRT mantenga un sitio web, o dedique una página dentro de un sitio web existente, en el que se ponga a disposición del público información general sobre los principales incidentes en materia de seguridad que afecten a las redes y sistemas de información acaecidos en toda la Unión, prestando una atención especial a los intereses y necesidades de las empresas. Conviene asimismo que los CSIRT que participen en dicha red faciliten con carácter voluntario la información que deba publicarse en ese sitio web, sin incluir información confidencial o delicada.

(41) Cuando la información se considere confidencial de conformidad con las normas nacionales y de la Unión en materia de confidencialidad empresarial, debe mantenerse ese carácter confidencial a la hora de desarrollar las actividades y cumplir los objetivos establecidos en la presente Directiva.

(42) Los ejercicios que simulan en tiempo real situaciones asociadas a un incidente son esenciales para comprobar el grado de preparación de los Estados miembros y su capacidad de cooperación por lo que respecta a la seguridad de las redes y sistemas de información. El ciclo de ejercicios denominado *CyberEurope*, coordinado por la ENISA con la participación de los Estados miembros, es una herramienta útil para hacer pruebas y elaborar recomendaciones sobre el modo de ir mejorando la gestión de incidentes a escala de la Unión. Considerando que, en la actualidad, los Estados miembros no están obligados a planificar ejercicios ni a participar en ellos, la creación de la red de CSIRT en virtud de la presente Directiva ha de permitirles participar en ejercicios basados en una planificación precisa y en decisiones estratégicas. El Grupo de cooperación establecido en virtud de la presente Directiva debe discutir sobre las decisiones estratégicas relativas a los ejercicios, en particular, aunque no exclusivamente, por lo que respecta a la regularidad de los mismos y a la concepción de las hipótesis. La ENISA, de conformidad con su mandato, debe apoyar la organización y realización de ejercicios a escala de la Unión, ofreciendo sus conocimientos especializados y su asesoramiento al Grupo de coordinación y a la red de CSIRT.

(43) El alcance mundial de los problemas que afectan a la seguridad de las redes y sistemas de información hace necesaria una mayor cooperación internacional para mejorar las normas de seguridad y el intercambio de información, y promover un planteamiento global común con respecto a las cuestiones de seguridad.

(44) La responsabilidad de velar por la seguridad de las redes y sistemas de información recae en gran medida en los operadores de servicios esenciales y los proveedores de servicios digitales. Debe fomentarse una cultura de gestión de riesgos que implique una evaluación del riesgo y la aplicación de medidas de seguridad adecuadas a los riesgos que hay que afrontar, y esta se debe desarrollar a través de requisitos normativos adecuados y prácticas sectoriales voluntarias. Asimismo, es indispensable sentar unas condiciones de igualdad dignas de confianza para garantizar el funcionamiento efectivo del Grupo de cooperación y la red de CSIRT y, por ende, la cooperación efectiva de todos los Estados miembros.

(45) La presente Directiva se aplica únicamente a las administraciones públicas que hayan sido identificadas como operadores de servicios esenciales. Por consiguiente, es responsabilidad de los Estados miembros garantizar la seguridad de las redes y sistemas de información de las administraciones públicas que no estén incluidas en el ámbito de aplicación de la presente Directiva.

(46) Entre las medidas de gestión del riesgo figuran aquellas cuya finalidad es determinar todo riesgo de incidentes, prevenir, detectar y gestionar incidentes y mitigar sus repercusiones. La seguridad de las redes y sistemas de información comprende la seguridad de los datos conservados, transmitidos y procesados.

(47) Las autoridades competentes deben seguir estando facultadas para adoptar directrices nacionales acerca de las circunstancias en las que los operadores de servicios esenciales deben notificar incidentes.

(48) Numerosas empresas de la Unión recurren para prestar sus propios servicios a proveedores de servicios digitales. Dado que algunos servicios digitales pueden representar un recurso importante para sus usuarios, incluidos los operadores de servicios esenciales, y dado que esos usuarios no siempre pueden recurrir a otras opciones, la presente Directiva debe aplicarse también a los proveedores de ese tipo de servicios. La seguridad, continuidad y fiabilidad del tipo de servicios digitales a que se refiere la presente Directiva tiene una importancia capital para el buen funcionamiento de numerosas empresas. La perturbación de un servicio digital puede impedir la prestación de otros servicios que dependen de él y afectar, por lo tanto, a actividades económicas y sociales fundamentales en la Unión. Por esa razón, ese tipo de servicios digitales puede tener una importancia capital para el correcto funcionamiento de las empresas que dependen de ellos, y también para la participación de estas en el mercado interior y en el comercio transfronterizo en toda la Unión. Esos proveedores de servicios digitales que están sujetos a la presente Directiva son aquellos que prestan servicios digitales de los que muchas empresas de la Unión dependen cada vez más.

(49) Los proveedores de servicios digitales deben garantizar un nivel de seguridad acorde con el grado de riesgo que se plantea para la seguridad de los servicios digitales que presten, teniendo cuenta la importancia de sus servicios para las operaciones de otras empresas de la Unión. En la práctica, el grado de riesgo para los operadores de servicios esenciales, que son a menudo esenciales para el mantenimiento de actividades sociales y económicas cruciales, es superior al que corresponde a los proveedores de servicios digitales. Por consiguiente, los proveedores de servicios digitales deben estar sujetos a requisitos de seguridad menos rigurosos. Los proveedores de servicios digitales deben seguir pudiendo tomar las medidas que consideren oportunas a fin de gestionar los riesgos que se planteen para la seguridad de sus redes y servicios de información. Debido a su carácter transfronterizo, los proveedores de servicios digitales deben estar sujetos a un planteamiento más armonizado a escala de la Unión. La especificación y aplicación de las medidas correspondientes debe verse facilitada mediante actos de ejecución.

(50) Aunque los fabricantes de equipos informáticos y quienes desarrollan programas informáticos no sean operadores de servicios esenciales ni proveedores de servicios digitales, sus productos facilitan la seguridad de las redes y sistemas de información. Desempeñan por ello un importante papel al permitir que los operadores de servicios esenciales y los proveedores de servicios digitales garanticen la seguridad de sus redes e infraestructuras de información. Estos equipos y programas informáticos están ya sujetos a las normas vigentes en materia de responsabilidad por los daños causados por productos defectuosos.

(51) Las medidas técnicas y de organización impuestas a los operadores de servicios esenciales y a los proveedores de servicios digitales no deben requerir que se diseñe, desarrolle o fabrique de una manera especial un determinado producto comercial de tecnología de la información y la comunicación.

(52) Los operadores de servicios esenciales y los proveedores de servicios digitales deben garantizar la seguridad de las redes y sistemas que utilicen. Se trata fundamentalmente de redes y sistemas privados gestionados por el personal informático interno o cuya seguridad se ha encomendado a empresas externas. Los requisitos en materia de seguridad y notificación han de aplicarse a los operadores de servicios esenciales y a los proveedores de servicios digitales pertinentes, independientemente de si se encargan ellos mismos del mantenimiento de sus redes y sistemas de información o lo subcontratan.

(53) Para no imponer una carga financiera y administrativa desproporcionada a los operadores de servicios esenciales y a los proveedores de servicios digitales, los requisitos han de ser proporcionados en relación con los riesgos que presenta la red y el sistema de información en cuestión, y tener en cuenta el estado de la técnica. En el caso de los proveedores de servicios digitales, esos requisitos no deben aplicarse ni a las microempresas ni a las pequeñas empresas.

(54) Las administraciones públicas de los Estados miembros que utilizan servicios ofrecidos por proveedores de servicios digitales, en particular servicios de computación en nube, pueden considerar conveniente exigir a los proveedores de tales servicios medidas de seguridad adicionales, más estrictas que las que dichos proveedores ofrecerían normalmente en cumplimiento de los requisitos de la presente Directiva. Han de poder hacerlo mediante obligaciones contractuales.

(55) Las definiciones de mercados digitales, motores de búsqueda en línea y servicios de computación en nube formuladas en la presente Directiva han de entenderse a los efectos específicos de esta, y sin perjuicio de cualquier otro instrumento.

(56) La presente Directiva no debe ser óbice para que los Estados miembros adopten medidas nacionales que obliguen a los organismos del sector público a garantizar unas condiciones de seguridad específicas cuando contraten servicios de computación en nube. Las medidas nacionales de ese tipo que se adopten deben aplicarse al organismo del sector público de que se trate, y no al proveedor de servicios de computación en nube.

57) Dadas las diferencias fundamentales existentes entre los operadores de servicios esenciales, en particular por su vinculación directa con infraestructuras físicas, y los proveedores de servicios digitales, en particular por su carácter transfronterizo, debe adoptarse en la presente Directiva un planteamiento diferenciado con respecto al nivel de armonización aplicable a esos dos grupos de entidades. Para los operadores de servicios esenciales, los Estados miembros deben poder identificar a los operadores correspondientes e imponerles requisitos más estrictos que los previstos en la presente Directiva. Los Estados miembros no deben identificar a los proveedores de servicios digitales, ya que la presente Directiva debe aplicarse a todos los proveedores de servicios digitales incluidos en su ámbito de aplicación. Por otra parte, la presente Directiva y los actos de ejecución que se adopten en virtud de esta deben garantizar un elevado nivel de armonización para los proveedores de servicios digitales respecto de los requisitos de seguridad y notificación. Ello debe permitir que los proveedores de servicios digitales sean tratados de manera uniforme en toda la Unión, de una manera proporcionada en relación con su naturaleza y con el grado de riesgo al que puedan tener que hacer frente.

(58) La presente Directiva no debe impedir que los Estados miembros impongan requisitos de seguridad y notificación a entidades que no sean proveedores de servicios digitales comprendidos en el ámbito de aplicación de la presente Directiva, sin perjuicio de las obligaciones de los Estados miembros en virtud del Derecho de la Unión.

(59) Las autoridades competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza. Antes de dar publicidad a los incidentes notificados a las autoridades competentes, es preciso sopesar debidamente el interés de los ciudadanos en ser informados sobre amenazas que en términos comerciales y de reputación puedan sufrir los operadores de servicios esenciales y los proveedores de servicios digitales que notifican incidentes. A la hora de cumplir sus obligaciones de notificación, las autoridades competentes y los CSIRT han de tener muy en cuenta la necesidad de mantener estrictamente confidencial la información sobre los puntos vulnerables del producto antes de dar a conocer las soluciones de seguridad adecuadas.

(60) Los proveedores de servicios digitales deben estar sujetos a un tipo de supervisión ligera, reactiva y *a posteriori*, justificada por la naturaleza de sus servicios y operaciones. La autoridad competente de que se trate debe, por tanto, intervenir únicamente cuando obtenga pruebas, por ejemplo del propio proveedor de servicios digitales, de otra autoridad competente, incluida una autoridad competente de otro Estado miembro, o de un usuario del servicio, de que un proveedor de servicios digitales no cumple los requisitos de la presente Directiva, en particular después de que se haya producido un incidente. Por consiguiente, la autoridad competente no debe tener la obligación general de supervisar a los proveedores de servicios digitales.

(61) Las autoridades competentes deben disponer de los medios necesarios para ejercer sus funciones, incluidas sus competencias para obtener información suficiente para evaluar el nivel de seguridad de las redes y sistemas de información.

(62) Los incidentes pueden ser consecuencia de actividades delictivas, cuya prevención, investigación y enjuiciamiento se ven facilitados por la coordinación y la cooperación entre los operadores de servicios esenciales, los proveedores de servicios digitales, las autoridades competentes y las autoridades policiales. Cuando se sospeche que un incidente guarda relación con actividades delictivas graves en virtud del Derecho de la Unión o nacional, los Estados miembros deben alentar a los operadores de servicios esenciales y a los proveedores de servicios digitales a notificar personalmente a las autoridades policiales competentes los incidentes de naturaleza presuntamente delictiva y grave. Es deseable que el Centro Europeo de Ciberdelincuencia de Europol (EC3) y la ENISA faciliten, en su caso, la coordinación entre las autoridades competentes y las autoridades policiales de los diferentes Estados miembros.

(63) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes y las autoridades responsables de la protección de datos han de cooperar e intercambiar la información sobre todos los asuntos pertinentes ante las violaciones de datos personales derivadas de incidentes.

(64) La competencia judicial respecto de los proveedores de servicios digitales debe atribuirse al Estado miembro en el que el operador tenga en la Unión su establecimiento principal, que corresponde en principio al lugar en el que el proveedor tiene su domicilio social en la Unión. Por establecimiento se entiende el ejercicio real y efectivo de una actividad mediante una organización estable. La forma jurídica de dicha organización, ya sea a través de una sucursal o una filial con personalidad jurídica, no es el factor determinante a este respecto. Este criterio no debe depender de que las redes y sistemas de información estén o no físicamente situados en un lugar determinado; la presencia y utilización de tales sistemas no pueden asimilarse por sí mismos a la existencia del mencionado establecimiento principal y no constituyen, por tanto, criterios para determinar el establecimiento principal.

(65) Cuando un proveedor de servicios digitales que no esté establecido en la Unión ofrezca servicios en ella, debe designar a un representante. Para determinar si dicho proveedor de servicios digitales ofrece servicios en la Unión, debe averiguarse si hay constancia de que el proveedor de servicios digitales tiene la intención de ofrecer servicios a personas de uno o varios Estados miembros. La simple accesibilidad en la Unión del sitio web del proveedor de servicios digitales o de un intermediario, o de una dirección de correo electrónico y otros datos de contacto, o el empleo de una lengua de uso común en el país tercero en que esté establecido el proveedor de servicios digitales, no basta para determinar dicha intención. No obstante, factores como el empleo de una lengua o una moneda, de uso común en uno o varios Estados miembros, con la posibilidad de encargar servicios en esa otra lengua, o la mención de clientes o usuarios que estén en la Unión, puede revelar que el proveedor de servicios digitales tiene la intención de ofrecer servicios en la Unión. El representante debe actuar por cuenta del proveedor de servicios digitales, y las autoridades competentes o los CSIRT han de poder ponerse en contacto con él. El representante debe haber sido designado expresamente mediante un mandato escrito del proveedor de servicios digitales que le autorice para actuar por cuenta de este en lo que respecta a las obligaciones del proveedor en virtud de la presente Directiva, también por lo que respecta a la obligación de notificación de incidentes.

(66) La normalización de los requisitos en materia de seguridad es un proceso impulsado por el mercado. Al objeto de garantizar una aplicación convergente de las normas de seguridad, los Estados miembros han de fomentar el cumplimiento de normas específicas o la conformidad con ellas para así lograr un elevado nivel de seguridad de las redes y sistemas de información en la Unión. La ENISA debe prestar asistencia a los Estados miembros ofreciéndoles asesoramiento y directrices. A tal fin, podría ser útil elaborar normas armonizadas, de conformidad con el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[1].

(67) Puede ocurrir que entidades no incluidas en el ámbito de aplicación de la presente Directiva sufran incidentes que tengan efectos significativos en los servicios que prestan. Cuando tales entidades consideren de interés público notificar que se han producido esos incidentes, deben poder hacerlo a título voluntario. Tales notificaciones solo deben ser tramitadas por la autoridad competente o por el CSIRT cuando su tramitación no suponga una carga desproporcionada o injustificada para los Estados miembros afectados.

[1] Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

(68) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución para establecer, por una parte, las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de cooperación y, por otra, los requisitos de seguridad y notificación aplicables a los proveedores de servicios digitales. Esas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[1]. Al adoptar actos de ejecución relacionados con las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de cooperación, la Comisión debe tener plenamente en cuenta el dictamen de la ENISA.

69) Al adoptar actos de ejecución relacionados con los requisitos de seguridad aplicables a los proveedores de servicios digitales, la Comisión debe tener plenamente en cuenta el dictamen de la ENISA y debe consultar a los interesados. Además, se alienta a la Comisión a que tenga en cuenta los siguientes ejemplos: por lo que respecta a la seguridad de los sistemas e instalaciones: la seguridad física y del entorno, la seguridad de abastecimiento, el control del acceso a las redes y sistemas de información y la integridad de las redes y sistemas de información; por lo que respecta a la gestión de incidentes: los procedimientos de gestión de incidentes, las capacidades de detección de incidentes, la información y comunicación sobre incidentes; por lo que respecta a la gestión de la continuidad de las actividades: la estrategia de continuidad de los servicios y los planes para contingencias y las capacidades de recuperación en caso de catástrofe; y, por lo que respecta a la supervisión, la auditoría y los ensayos: las políticas de supervisión y registro, la planificación de contingencias durante los ejercicios, los ensayos con las redes y sistemas de información, las evaluaciones de seguridad y el control del cumplimiento de la normativa.

[1] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(70) Al aplicar la presente Directiva, la Comisión debe mantener contactos, según corresponda, con los comités sectoriales y organismos pertinentes establecidos a escala de la Unión en los ámbitos a los que se aplica la presente Directiva.

(71) La Comisión debe revisar periódicamente lo dispuesto en la presente Directiva, en consulta con los interesados, en particular para determinar si se precisa alguna modificación a raíz de cambios en la situación social, política, de la tecnología o el mercado.

(72) El intercambio de información sobre riesgos e incidentes que ha de llevarse a cabo en el Grupo de cooperación y la red de los CSIRT, y el cumplimiento de la obligación de notificar los incidentes a las autoridades nacionales competentes o a los CSIRT, pueden hacer necesario el tratamiento de datos personales. Dicho tratamiento debe cumplir lo dispuesto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo[1] y en el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo[2]. Al aplicar la presente Directiva, se debe aplicar, según corresponda, el Reglamento (CE) n.º 1049/2001,[3].

(73) El Supervisor Europeo de Protección de Datos, consultado de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, emitió un dictamen el 14 de junio de 2013[4].

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

2 Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

3 Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

4 DO C 32 de 4.2.2014, p. 19.

(74) Dado que el objetivo de la presente Directiva, a saber, garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dicho objetivo.

(75) La presente Directiva observa los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea, en particular, el derecho al respeto de la vida privada y las comunicaciones, el derecho a la protección de los datos de carácter personal, la libertad de empresa, el derecho a la propiedad, el derecho a una tutela judicial efectiva y el derecho a ser oído. La presente Directiva debe aplicarse de conformidad con estos derechos y principios.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior.

2. A tal fin, la presente Directiva:

   a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

   b) crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

   c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «Computer Security Incident Response Teams») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

   d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

e) establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

3. Los requisitos de seguridad y notificación previstos en la presente Directiva no serán aplicables a las empresas que están sujetas a los requisitos de los artículos 13 *bis y 1*3 *ter* de la Directiva 2002/21/CE ni a los proveedores de servicios de confianza sujetos a los requisitos del artículo 19 del Reglamento (UE) n.º 910/2014.

4. La presente Directiva se entenderá sin perjuicio de la Directiva 2008/114/CE[1] y las Directivas 2011/193/UE[2] y 2013/40/UE[3] del Parlamento Europeo y del Consejo.

5. Sin perjuicio de lo dispuesto en el artículo 346 del TFUE, la información que se considere confidencial de acuerdo con las normas de la Unión y nacionales, como las normas sobre confidencialidad empresarial, se intercambiará con la Comisión y otras autoridades competentes únicamente cuando tal intercambio sea necesario a efectos de la aplicación de la presente Directiva. La información que se intercambie se limitará a aquella que resulte pertinente y proporcionada para la finalidad del intercambio. Dicho intercambio de información preservará la confidencialidad de esta y protegerá los intereses de seguridad y comerciales de los operadores de servicios esenciales y de los proveedores de servicios digitales.

---

1 Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

2 Directiva 2011/93/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo (DO L 335 de 17.12.2011, p. 1).

3 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DO L 218 de 14.8.2013, p. 8).

6. La presente Directiva se entenderá sin perjuicio de las acciones emprendidas por los Estados miembros para salvaguardar sus funciones estatales esenciales, en particular para salvaguardar la seguridad nacional, incluidas las acciones que protejan la información cuya revelación los Estados miembros consideren contraria a los intereses esenciales de su seguridad, y para mantener el orden público, en particular para permitir la investigación, la detección y el enjuiciamiento de infracciones penales.

7. Se aplicará lo dispuesto en un acto jurídico sectorial de la Unión, cuando este requiera que los operadores de servicios esenciales o los proveedores de servicios digitales garanticen la seguridad de sus redes y sistemas de información o notifiquen incidentes, siempre que dichos requisitos tengan al menos un efecto equivalente al de las obligaciones establecidas en la presente Directiva.

Artículo 2

Tratamiento de datos personales

1. El tratamiento de datos personales conforme a la presente Directiva se llevará a cabo de conformidad con la Directiva 95/46/CE.

2. El tratamiento de datos personales por las instituciones y los órganos de la Unión conforme a la presente Directiva se llevará a cabo de conformidad con el Reglamento (CE) n.º 45/2001.

Artículo 3

Armonización mínima

Sin perjuicio de lo dispuesto en el artículo 16, apartado 10, y de sus obligaciones en virtud del Derecho de la Unión, los Estados miembros podrán adoptar o mantener disposiciones con el objeto de alcanzar un mayor nivel de seguridad de las redes y sistemas de información.

Artículo 4

Definiciones

A los efectos de la presente Directiva, se entenderá por:

1) «redes y sistemas de información»:

   a) una red de comunicaciones electrónicas en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE,

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

   c) los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

2) «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;

3) «estrategia nacional de seguridad de las redes y sistemas de información»: un marco que proporciona prioridades y objetivos estratégicos de seguridad de las redes y sistemas de información a escala nacional;

4) «operador de servicios esenciales»: una entidad pública o privada de uno de los tipos que figuran en el anexo II, que reúna los criterios establecidos en el artículo 5, apartado 2;

5) «servicio digital»: un servicio en el sentido del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo[1] que sea de uno de los tipos que figuran en el anexo III;

6) «proveedor de servicios digitales»: toda persona jurídica que preste un servicio digital;

7) «incidente»: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información;

8) «gestión de incidentes»: todos los procedimientos seguidos para detectar, analizar, analizar y limitar un incidente y responder ante este;

[1] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

9) «riesgo»: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información;

10) «representante»: toda persona física o jurídica establecida en la Unión que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión, al que puede dirigirse una autoridad competente nacional o un CSIRT en sustitución del proveedor de servicios digitales, en lo que respecta a las obligaciones del proveedor de servicios digitales en virtud de la presente Directiva;

11) «norma»: una norma en el sentido del artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012;

12) «especificación»: una especificación técnica en el sentido del artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012;

13) «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 solo permite interconectar sistemas autónomos; un IXP no requiere que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, ni modifica ni interfiere de otra forma en dicho tráfico;

14) «servidor de sistema de nombres de dominio ("DNS", por sus siglas en inglés de "Domain Name System")»: un sistema de nombres de dominio distribuido jerárquicamente en una red que recibe consultas sobre nombres de dominio;

15) «proveedor de servicios de DNS»: una entidad que presta servicios de DNS en Internet;

16) «registro de nombres de dominio de primer nivel»: una entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel;

17) «mercado en línea»: un servicio digital que permite a los consumidores o a los comerciantes, como se definen respectivamente en el artículo 4, apartado 1, letra a) y letra b), de la Directiva 2013/11/UE del Parlamento Europeo y del Consejo[1], celebrar contratos de compraventa o de servicios en línea con comerciantes, ya sea en el sitio web del mercado en línea o en un sitio web de un comerciante que utilice servicios informáticos proporcionados por el mercado en línea;

18) «motor de búsqueda en línea»: un 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 cualquiera 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;

19) «servicio de computación en nube»: un servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir;

Artículo 5

Identificación de operadores de servicios esenciales

1. A más tardar el… [*27 meses después de la fecha de entrada en vigor de la presente Directiva*], los Estados miembros identificarán a los operadores de servicios esenciales establecidos en su territorio para cada sector y subsector mencionados en el anexo II.

[1] Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE (Directiva sobre resolución alternativa de litigios en materia de consumo) (DO L 165 de 18.6.2013, p. 63).

2. Los criterios para la identificación de operadores de servicios esenciales a que se refiere el artículo 4, punto 4, son los siguientes:

a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;

b) la prestación de dicho servicio depende de las redes y sistemas de información; y

c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio.

3. A efectos del apartado 1, cada Estado miembro establecerá una lista de los servicios mencionados en el apartado 2, letra a).

4. A efectos del apartado 1, cuando una entidad preste un servicio tal como se contempla en el apartado 2, letra a), en dos o más Estados miembros, estos se consultarán entre ellos. Dicha consulta tendrá lugar antes de se adopte una decisión sobre la identificación.

5. Los Estados miembros revisarán con regularidad, y al menos cada dos años a partir del … [*21 meses después de la entrada en vigor de la presente Directiva*], la lista de operadores de servicios esenciales identificados y la actualizarán cuando proceda.

6. La misión del Grupo de cooperación será, de conformidad con las funciones contempladas en el artículo 11, apoyar a los Estados miembros para que adopten un planteamiento coherente en el proceso de identificación de los operadores de servicios esenciales.

7. A efectos de la revisión a que se refiere el artículo 23, a más tardar el… [*27 meses después de la fecha de entrada en vigor de la presente Directiva*], y cada dos años a partir de entonces, los Estados miembros remitirán a la Comisión la información necesaria para que pueda evaluar la aplicación de la presente Directiva, en particular la coherencia de los planteamientos de los Estados miembros respecto a la identificación de los operadores de servicios esenciales. Dicha información deberá contener, como mínimo:

a) las medidas nacionales que permitan identificar operadores de servicios esenciales;

b) la lista de servicios contemplada en el apartado 3;

c) el número de operadores de servicios esenciales identificados para cada uno de los sectores que figuran en el anexo II y una indicación de su importancia en relación con dicho sector;

d) los umbrales, cuando existan, para determinar el nivel de suministro pertinente en función del número de usuarios que confían en ese servicio a que hace referencia el artículo 6, apartado 1, letra a), o la importancia de ese operador concreto de servicios esenciales a que hace referencia el artículo 6, apartado1, letra f).

A fin de contribuir a que se aporte información comparable, la Comisión, teniendo en cuenta en la mayor medida posible el dictamen de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), podrá adoptar directrices técnicas adecuadas sobre parámetros para la información contemplada en el presente apartado.

Artículo 6

Efecto perturbador significativo

1. A la hora de determinar la importancia de un efecto perturbador tal como se indica en el artículo 5 apartado 2, letra c), los Estados miembros tendrán en cuenta al menos los siguientes factores intersectoriales:

   a) el número de usuarios que confían en los servicios prestados por la entidad de que se trate;

   b) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad;

   c) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública;

   d) la cuota de mercado de la entidad;

   e) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente;

   f) la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio.

2. A fin de determinar si un incidente podría tener efectos perturbadores significativos, los Estados miembros también tendrán en cuenta factores específicos del sector, cuando proceda.

CAPÍTULO II
MARCOS NACIONALES DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

Artículo 7

Estrategia nacional de seguridad de las redes y sistemas de información

1. Cada Estado miembro adoptará una estrategia nacional de seguridad de las redes y sistemas de información que establezca los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información y que cubra al menos los sectores que figuran en el anexo II y los servicios que figuran en el anexo III. La estrategia nacional de seguridad de las redes y sistemas de información abordará, en particular, las cuestiones siguientes:

   a) los objetivos y prioridades de la estrategia nacional de seguridad de las redes y sistemas de información;

   b) un marco de gobernanza para lograr los objetivos y las prioridades de la estrategia nacional de seguridad de las redes y sistemas de información, incluidas las funciones y responsabilidades de las instituciones públicas y de los demás agentes pertinentes;

   c) la identificación de medidas sobre preparación, respuesta y recuperación, incluida la cooperación entre los sectores público y privado;

d) una indicación de los programas de educación, concienciación y formación relacionados con la estrategia nacional de seguridad de las redes y sistemas de información;

e) una indicación de los programas de investigación y desarrollo relacionados con la estrategia nacional de seguridad de las redes y sistemas de información;

f) un plan de evaluación de riesgos para identificar riesgos;

g) una lista de los diversos agentes que participan en la ejecución de la estrategia de seguridad de las redes y sistemas de información.

2. Los Estados miembros podrán solicitar la asistencia de la ENISA a la hora de elaborar estrategias nacionales de seguridad de las redes y sistemas de información.

3. Los Estados miembros comunicarán sus estrategias nacionales de seguridad de las redes y sistemas de información a la Comisión en el plazo de tres meses a partir de su adopción. Al hacerlo, los Estados miembros podrán excluir elementos de la estrategia relacionados con la seguridad nacional.

Artículo 8

Autoridades nacionales competentes y punto de contacto único

1. Cada Estado miembro designará una o más autoridades nacionales competentes en materia de seguridad de las redes y sistemas de información («autoridad competente») que cubra al menos los sectores que figuran en el anexo II y los servicios que figuran en el anexo III. Los Estados miembros podrán asignar esta función a una autoridad o autoridades existentes.

2. Las autoridades competentes supervisarán la aplicación de la presente Directiva a escala nacional.

3 Cada Estado miembro designará un punto de contacto único en materia de seguridad de las redes y sistemas de información (en lo sucesivo, «punto de contacto único»). Los Estados miembros podrán asignar esta función a una autoridad existente. Si un Estado miembro designa únicamente una autoridad competente, dicha autoridad también será el punto de contacto único.

4 El punto de contacto único ejercerá una función de enlace para garantizar la cooperación transfronteriza entre las autoridades de los Estados miembros y con las autoridades competentes en otros Estados miembros y con el Grupo de cooperación a que se refiere el artículo 11 y la red de CSIRT a que se refiere el artículo 12.

5. Los Estados miembros velarán por que las autoridades competentes y los puntos de contacto únicos dispongan de recursos adecuados para ejercer las funciones que les son asignadas de forma efectiva y eficiente y cumplir así los objetivos de la presente Directiva. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de los representantes designados en el Grupo de cooperación

6. Las autoridades competentes y los puntos de contacto únicos, cuando proceda y de conformidad con el Derecho nacional, consultarán a las autoridades policiales nacionales competentes y a las autoridades nacionales responsables de la protección de datos y cooperarán con ellas.

7. Los Estados miembros notificarán sin dilación a la Comisión la autoridad competente y el punto de contacto único que hayan designado, sus funciones y cualquier cambio posterior que se introduzca. Los Estados miembros harán pública su designación de la autoridad competente y el punto de contacto único. La Comisión publicará la lista de puntos de contacto únicos designados.

Artículo 9

Equipos de respuesta a incidentes de seguridad informática (CSIRT)

1. Cada Estado miembro designará uno o varios CSIRT que cumplan los requisitos establecidos en el anexo I, punto 1, que cubran al menos los sectores que figuran en el anexo II y los tipos de servicios digitales que figuran en el anexo III, responsables de la gestión de incidentes y riesgos de conformidad con un procedimiento claramente definido. Podrá crearse un CSIRT en el marco de una autoridad competente.

2. Los Estados miembros velarán por que los CSIRT designados dispongan de recursos adecuados para ejercer eficazmente sus funciones, tal como se establece en el anexo I, punto 2.

   Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT a que hace referencia el artículo 12.

3. Los Estados miembros velarán por que sus CSIRT designados tengan acceso a una infraestructura de comunicación e información apropiada, segura y resiliente a escala nacional.

4. Los Estados miembros informarán a la Comisión del mandato y de los elementos principales del proceso de gestión de incidentes de sus CSIRT.

5. Los Estados miembros podrán solicitar la asistencia de la ENISA a la hora de crear CSIRT nacionales.

Artículo 10

Cooperación a escala nacional

1. Cuando sean distintos, la autoridad competente, el punto de contacto único y los CSIRT del mismo Estado miembro cooperarán respecto al cumplimiento de las obligaciones establecidas en la presente Directiva.

2. Los Estados miembros velarán por que las autoridades competentes o los CSIRT reciban las notificaciones sobre incidentes presentadas en el marco de la presente Directiva. Cuando un Estado miembro decida que los CSIRT no recibirán notificaciones, se dará a estos últimos, en la medida necesaria para que cumplan sus funciones, el acceso a los datos sobre incidentes notificados por los operadores de servicios esenciales con arreglo al artículo 14, apartados 3 y 5, o por los proveedores de servicios digitales con arreglo al artículo 16, apartados 3 y 6.

3. Los Estados miembros velarán por que las autoridades competentes o los CSIRT informen a los puntos de contacto únicos sobre las notificaciones de incidentes presentadas en el marco de la presente Directiva.

   A más tardar el … *[24 meses después de la entrada en vigor de la presente Directiva]*, y una vez al año a partir de entonces, el punto de contacto único presentará al Grupo de cooperación un informe resumido sobre las notificaciones recibidas, con mención del número de notificaciones y de la naturaleza de los incidentes notificados, así como de las acciones emprendidas de conformidad con el artículo 14, apartados 3 y 5*,* y el artículo 16, apartados 3 y 6.

CAPÍTULO III
COOPERACIÓN

Artículo 11

Grupo de cooperación

1. Se establece un Grupo de cooperación a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar confianza y seguridad, y a fin de alcanzar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

   El Grupo de cooperación ejercerá sus funciones con arreglo a los programas de trabajo bienales a que se refiere el apartado 3, párrafo segundo.

2. El Grupo de cooperación estará formado por representantes de los Estados miembros, la Comisión y la ENISA.

   Cuando proceda, el Grupo de cooperación podrá invitar a representantes de los interesados pertinentes a que participen en su labor.

   La Comisión se hará cargo de la secretaría.

3. El Grupo de cooperación ejercerá las siguientes funciones:

   a) proporcionar orientación estratégica para las actividades de la red de CSIRT establecida en virtud del artículo 12;

b) intercambiar buenas prácticas cuando se intercambie información relativa a la notificación de incidentes tal como se contempla en el artículo 14, apartados 3 y 5, y en el artículo 16, apartados 3 6;

c) intercambiar buenas prácticas entre los Estados miembros y, en colaboración con la ENISA, asistir a los Estados miembros en el desarrollo de capacidades para garantizar la seguridad de las redes y sistemas de información;

d) discutir sobre las capacidades y la preparación de los Estados miembros, evaluar voluntariamente las estrategias nacionales de seguridad de las redes y sistemas de información y la eficacia de los CSIRT e identificar las buenas prácticas;

e) intercambiar información y buenas prácticas sobre concienciación y formación;

f) intercambiar información y buenas prácticas sobre investigación y desarrollo en materia seguridad de las redes y sistemas de información;

g) cuando proceda, intercambiar experiencias sobre asuntos relativos a seguridad de las redes y sistemas de información con las instituciones, órganos y organismos de la Unión competentes;

h) discutir sobre las normas y especificaciones a que hace referencia el artículo 19 con los representantes de los organismos europeos de normalización pertinentes;

i) recopilar información de buenas prácticas sobre los riesgos e incidentes que afecten a las redes y sistemas de información;

j) examinar anualmente los informes resumidos que menciona el artículo 10, apartado 3, párrafo segundo;

k) discutir sobre el trabajo emprendido con respecto a ejercicios relativos a la seguridad de las redes y sistemas de información, programas educativos y formación, incluido el trabajo realizado por la ENISA;

l) con la asistencia de la ENISA, intercambiar buenas prácticas con respecto a la identificación de operadores de servicios esenciales por parte de los Estados miembros, en particular en relación con las dependencias transfronterizas, en lo que atañe a riesgos e incidentes;

m) discutir sobre las modalidades para informar sobre notificaciones de incidentes tal como se contempla en los artículos 14 y 16;

A más tardar el … *[18 meses después de la entrada en vigor de la presente Directiva]* y cada dos años a partir de entonces, el Grupo de cooperación establecerá un programa de trabajo sobre las acciones que deben emprenderse para realizar sus objetivos y funciones, que serán coherentes con los objetivos de la presente Directiva.

4. A efectos de la revisión a que se refiere el artículo 23, a más tardar el … *[24 meses después de la entrada en vigor de la presente Directiva]*, y cada año y medio a partir de entonces, el Grupo de cooperación elaborará un informe para valorar la experiencia adquirida con la cooperación estratégica contemplada en el presente artículo.

5. La Comisión adoptará actos de ejecución para establecer las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de cooperación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 22, apartado 2.

A efectos del párrafo primero, la Comisión presentará al Comité el primer proyecto de acto de ejecución a que se refiere el artículo 22, apartado 1, a más tardar el … *[seis meses después de la entrada en vigor de la presente Directiva].*

Artículo 12
Red de CSIRT

1. A fin de contribuir a desarrollar la confianza y la seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz, se establece una red de CSIRT nacionales.

2. La red de CSIRT estará formada por representantes de los CSIRT de los Estados miembros. La Comisión participará en la red de CSIRT en calidad de observador. La ENISA se hará cargo de la secretaría y apoyará activamente la cooperación entre los CSIRT.

3. La red de CSIRT desempeñará los siguientes cometidos:

   a) intercambiar información sobre servicios, operaciones y capacidades de cooperación de los CSIRT;

   b) a instancias de un representante de un CSIRT de un Estado miembro que pueda verse afectado por un incidente, intercambiar y discutir sobre información sensible de carácter no comercial relacionada con ese incidente y los riesgos asociados; no obstante, todo Estado miembro podrá negarse a contribuir a dicha discusión si existe riesgo de perjuicio para la investigación del incidente;

c) intercambiar y proporcionar voluntariamente información no confidencial sobre incidentes concretos;

d) a instancias de un representante de un CSIRT de un Estado miembro, discutir y, cuando sea posible, determinar una respuesta coordinada a un incidente que se haya identificado dentro del ámbito de competencias de ese Estado miembro;

e) prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos sobre la base de su asistencia mutua voluntaria;

f) discutir, explorar e identificar más formas de cooperación operativa, incluidas las relacionadas con:

   i) categorías de riesgos e incidentes,

   ii) alertas tempranas,

   iii) asistencia mutua,

   iv) principios y modalidades de coordinación, cuando los Estados miembros respondan ante incidentes y riesgos transfronterizos de seguridad de las redes y sistemas de información;

g) informar al Grupo de cooperación sobre sus actividades y sobre las formas adicionales de cooperación operativa sobre las que se haya discutido conforme al apartado 3, letra f), y solicitar directrices a este respecto;

h) discutir sobre la experiencia adquirida a partir de los ejercicios relativos a la seguridad de las redes y sistemas de información, entre ellas las organizadas por la ENISA;

i) a instancias de un CSIRT determinado, analizar las capacidades y la preparación de ese mismo CSIRT;

j) publicar directrices para facilitar la convergencia de prácticas operativas con respecto a la aplicación de lo dispuesto en el presente artículo en lo que atañe a la cooperación operativa.

4. A efectos de la revisión que contempla el artículo 23, a más tardar el … *[24 meses después de la entrada en vigor de la presente Directiva]*, y **cada año y medio** a partir de entonces, la red de CSIRT elaborará un informe en el que se examine la experiencia adquirida a través de la cooperación operativa, en particular las conclusiones y recomendaciones, practicada con arreglo al presente artículo. Dicho informe también se enviará al Grupo de cooperación.

5. La red de CSIRT establecerá su reglamento interno.

Artículo 13

Cooperación internacional

La Unión podrá celebrar, de conformidad con el artículo 218 del TFUE, acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades del Grupo de cooperación. En tales acuerdos se tendrá en cuenta la necesidad de garantizar una protección de datos adecuada.

CAPÍTULO IV
SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN DE LOS OPERADORES DE SERVICIOS ESENCIALES

Artículo 14

Requisitos en materia de seguridad y notificación de incidentes

1. Los Estados miembros velarán por que los operadores de servicios esenciales tomen las 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 que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado.

2. Los Estados miembros velarán por que los operadores de servicios esenciales tomen medidas adecuadas para prevenir y reducir al mínimo los efectos de los incidentes que afecten la seguridad de las redes y sistemas de información utilizados para la prestación de tales servicios esenciales con el objeto de garantizar su continuidad.

3 Los Estados miembros velarán por que los operadores de servicios esenciales notifiquen sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan. Las notificaciones incluirán información que permita a la autoridad competente o al CSIRT determinar cualquier efecto transfronterizo del incidente. La notificación no sujetará al notificante a una mayor responsabilidad.

4. A fin de determinar la importancia de los efectos de un incidente, se tendrán en cuenta, en particular, los siguientes parámetros:

   a) el número de usuarios afectados por la perturbación del servicio esencial;

   b) la duración del incidente;

   c) la extensión geográfica con respecto a la zona afectada por el incidente.

5. Sobre la base de la información proporcionada en la notificación por el operador de servicios esenciales, la autoridad competente o el CSIRT informará al otro u otros Estados miembros afectados acerca de si el incidente tiene efectos significativos en la continuidad de los servicios esenciales en dicho Estado miembro. Al hacerlo, la autoridad competente o el CSIRT, de conformidad con el Derecho de la Unión o con la legislación nacional acorde con el Derecho de la Unión, mantendrán la seguridad y los intereses comerciales del operador de servicios esenciales así como la confidencialidad de la información proporcionada en su notificación.

   Cuando las circunstancias lo permitan, la autoridad competente o el CSIRT proporcionarán al operador de servicios esenciales notificante la información pertinente con respecto al seguimiento de la notificación de un incidente, por ejemplo la información que podría facilitar la gestión eficaz del incidente.

   A instancias de la autoridad competente o del CSIRT, el punto de contacto único remitirá las notificaciones contempladas en el párrafo primero a los puntos de contacto únicos de otros Estados miembros afectados.

6. Después de consultar al operador de servicios esenciales notificante, la autoridad competente o el CSIRT podrán informar al público sobre determinados incidentes, cuando la concienciación pública sea necesaria para evitar un incidente o gestionar uno que ya se haya producido.

7. Las autoridades competentes que actúen juntas dentro del Grupo de cooperación podrán elaborar y adoptar directrices relativas a las circunstancias en las que se exija a los operadores de servicios esenciales que notifiquen incidentes, en particular sobre los parámetros para determinar la importancia de los efectos de un incidente a que se refiere el apartado 4.

Artículo 15

Aplicación y observancia

1. Los Estados miembros velarán por que las autoridades competentes dispongan de las competencias y los medios necesarios para evaluar el cumplimiento por los operadores de servicios esenciales de las obligaciones que les impone el artículo 14 y los efectos que tengan sobre la seguridad de las redes y sistemas de información.

2. Los Estados miembros velarán por que la autoridad competente disponga de las competencias y los medios para exigir a los operadores de servicios esenciales que proporcionen:

   a) la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre las políticas de seguridad;

b) pruebas de la aplicación efectiva de las políticas de seguridad, como el resultado de las auditorías de seguridad realizadas por la autoridad competente o por un auditor cualificado y, en este último caso, que pongan a disposición de la autoridad competente el resultado de dicha auditoría y, en particular, las pruebas subyacentes.

Al exigir dicha información o pruebas, las autoridades competentes indicarán la finalidad de su petición y especificarán la información exigida.

3. Tras la evaluación de la información o del resultado de las auditorías de seguridad a que se refiere el apartado 2, la autoridad competente podrá impartir instrucciones vinculantes a los operadores de servicios esenciales para subsanar las deficiencias detectadas.

4. La autoridad competente cooperará estrechamente con las autoridades responsables de la protección de datos a la hora de hacer frente a incidentes que den lugar a violaciones de datos personales.

CAPÍTULO V
SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN DE LOS PROVEEDORES DE SERVICIOS DIGITALES

Artículo 16

Requisitos en materia de seguridad y notificación de incidentes

1. Los Estados miembros velarán por que los proveedores de servicios digitales determinen y adopten medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que se utilizan en el marco de la oferta de servicios en la Unión a que se refiere el anexo III. Habida cuenta de los avances técnicos, dichas medidas garantizarán un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado, y tendrán en cuenta lo siguiente:

   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.

2. Los Estados miembros velarán por que los proveedores de servicios digitales adopten medidas para prevenir y reducir al mínimo el impacto de los incidentes que afectan a la seguridad de sus redes y sistemas de información en los servicios a que se refiere el anexo III que se ofrecen en la Unión, a fin de garantizar la continuidad de dichos servicios.

3. Los Estados miembros velarán por que los proveedores de servicios digitales notifiquen sin dilación indebida a la autoridad competente o al CSIRT cualquier incidente que tenga un impacto significativo en la prestación de uno de los servicios a que se refiere el anexo III que ellos ofrezcan en la Unión. Las notificaciones incluirán la información necesaria para que la autoridad competente o el CSIRT puedan determinar la importancia de cualquier impacto transfronterizo. La notificación no sujetará al notificante a una mayor responsabilidad.

4. Para determinar si el impacto de un incidente es significativo se tendrán en cuenta, en particular, los siguientes parámetros:

   a) el número de usuarios afectados por el incidente, en particular los usuarios que dependen del servicio para la prestación de sus propios servicios;

   b) la duración del incidente;

   c) la extensión geográfica con respecto a la zona afectada por el incidente;

   d) el grado de perturbación del funcionamiento del servicio;

   e) el alcance del impacto sobre las actividades económicas y sociales.

La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente en función de los parámetros que se indican en el párrafo primero.

5. Cuando un operador de servicios esenciales dependa de un proveedor tercero de servicios digitales para la prestación de un servicio que es esencial para el mantenimiento de actividades sociales y económicas fundamentales, dicho operador notificará cualquier efecto significativo en la continuidad de los servicios esenciales causado por un incidente que afecte al proveedor de servicios digitales.

6. Cuando proceda, y en particular si el incidente mencionado en el apartado 2 afecta a dos o varios Estados miembros, la autoridad o el CSIRT al que se haya notificado el incidente informará del mismo a los demás Estados miembros afectados. Al hacerlo, las autoridades competentes, el CSIRT y los puntos de contacto únicos preservarán, de conformidad con el Derecho de la Unión o de la legislación nacional acorde con el Derecho de la Unión, la seguridad y los intereses comerciales del proveedor de servicios digitales así como la confidencialidad de la información facilitada.

7. Tras consultar al proveedor de servicios digitales afectado, la autoridad competente o el CSIRT al que se le haya notificado el incidente y, en su caso, las autoridades o el CSIRT de los demás Estados miembros afectados, podrán informar al público de determinados incidentes o exigir al proveedor de servicios digitales que lo haga, cuando el conocimiento del público sea necesario para evitar un incidente o hacer frente a un incidente en curso, o cuando la divulgación de un incidente redunde en interés público.

8. La Comisión adoptará actos de ejecución en los que se especifiquen más los elementos a que se refiere el apartado 1 y los parámetros enumerados en el apartado 4 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 22, apartado 2, a más tardar el … *[un año después de la entrada en vigor de la presente Directiva]*.

9. La Comisión podrá adoptar actos de ejecución por los que se establezcan los formatos y procedimientos aplicables a los requisitos de notificación. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 22, apartado 2.

10. Sin perjuicio de lo dispuesto en el artículo 1, apartado 6, los Estados miembros no impondrán nuevos requisitos de seguridad o de notificación a los proveedores de servicios digitales.

11. El presente capítulo no se aplicará a las microempresas y pequeñas empresas tal como se definen en la Recomendación 2003/361/CE[1] de la Comisión.

Artículo 17

Aplicación y observancia

1. Los Estados miembros velarán por que las autoridades competentes adopten medidas, si fuera necesario, mediante actividades de supervisión *a posteriori*, cuando tengan pruebas de que un proveedor de servicios digitales no cumple los requisitos establecidos en el artículo 16. Dichas pruebas podrán ser presentadas por la autoridad competente de otro Estado miembro en el que se presta el servicio.

[1] Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

2. A efectos del apartado 1, las autoridades competentes contarán con las atribuciones y medios necesarios para exigir a los proveedores de servicios digitales que:

a) proporcionen la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre las políticas de seguridad;

b) subsanen cualquier incumplimiento de los requisitos establecidos en el artículo 16.

3. Si un proveedor de servicios digitales tiene su establecimiento principal o un representante en un Estado miembro, pero sus redes y sistemas de información en otro u otros Estados miembros, la autoridad competente del Estado miembro en el que se encuentre su establecimiento principal o el representante y las autoridades competentes de esos otros Estados miembros cooperarán entre sí y se asistirán mutuamente cuando sea necesario. Dicha asistencia y cooperación podrá abarcar el intercambio de información entre las autoridades competentes de que se trate y las peticiones de que se adopten las medidas de supervisión contempladas en el apartado 2.

Artículo 18

Jurisdicción y territorialidad

1. A efectos de la presente Directiva, un proveedor de servicios digitales se considerará sometido a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal. Se considerará que un proveedor de servicios digitales tiene su establecimiento principal en un Estado miembro cuando su domicilio social se encuentre en ese Estado miembro.

2. Un proveedor de servicios digitales que no está establecido en la Unión, pero que ofrece servicios que figuran en el anexo III en la Unión, designará un representante en ella. El representante se establecerá en uno de aquellos Estados miembros en los que se ofrecen los servicios. Un proveedor de servicios digitales se considerará sometido a la jurisdicción del Estado miembro en el que se encuentre establecido su representante.

3. La designación de un representante por el proveedor de servicios digitales se entenderá sin perjuicio de las acciones legales que pudieran emprenderse contra el propio proveedor de servicios digitales.

CAPÍTULO VI
NORMALIZACIÓN Y NOTIFICACIÓN VOLUNTARIA

Artículo 19
Normalización

1. A fin de promover una aplicación convergente de lo dispuesto en el artículo 14, apartados 1 y 2, y en el artículo 16, apartados 1 y 2, los Estados miembros fomentarán, sin imponer ni favorecer el uso de un tipo específico de tecnología, la utilización de normas y especificaciones aceptadas a nivel europeo o internacionalmente que sean pertinentes en materia de seguridad de las redes y sistemas de información.

2. La ENISA, en colaboración con los Estados miembros, elaborará directrices y orientaciones relativas a las áreas técnicas que deban examinarse en relación con el apartado 1, así como en relación con las normas ya existentes, en particular las normas nacionales de los Estados miembros que permitirían cubrir esas áreas.

Artículo 20

Notificación voluntaria

1. Sin perjuicio de lo dispuesto en el artículo 3, las entidades que no hayan sido identificadas como operadores de servicios esenciales y no sean proveedores de servicios digitales podrán notificar voluntariamente los incidentes que tengan efectos significativos en la continuidad de los servicios que prestan.

2. Cuando tramiten las notificaciones, los Estados miembros actuarán de conformidad con el procedimiento establecido en el artículo 14. Los Estados miembros podrán dar prioridad a la tramitación de notificaciones obligatorias sobre las notificaciones voluntarias. Las notificaciones voluntarias se tramitarán únicamente cuando dicha tramitación no suponga una carga desproporcionada o indebida para los Estados miembros de que se trate.

   La notificación voluntaria no dará lugar a la imposición a la entidad notificante de obligaciones a las que no estaría sujeta de no haberse producido dicha notificación.

CAPÍTULO VII
DISPOSICIONES FINALES

Artículo 21

Sanciones

Los Estados miembros establecerán el régimen de sanciones aplicables en caso de incumplimiento de las disposiciones nacionales aprobadas al amparo de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su aplicación. Tales sanciones serán efectivas, proporcionadas y disuasorias. Los Estados miembros comunicarán ese régimen y esas medidas a la Comisión, a más tardar el … *[21 meses después de la entrada en vigor de la presente Directiva]*, y le notificarán sin demora toda modificación posterior de las mismas.

Artículo 22

Procedimiento de comité

1. La Comisión estará asistida por el Comité de Seguridad de las Redes y Sistemas de Información. Dicho Comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 23

Revisión

1. A más tardar el … *[33 meses después de la entrada en vigor de la presente Directiva]*, la Comisión presentará un informe al Parlamento Europeo y al Consejo en el que se examine la coherencia de los planteamientos adoptados por los Estados miembros respecto a la identificación de los operadores de servicios esenciales.

2. La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. A tal efecto y con vistas a incrementar la cooperación estratégica y operativa, la Comisión tendrá en cuenta los informes del Grupo de cooperación y de la red de CSIRT sobre la experiencia adquirida a nivel estratégico y operativo. En su revisión, la Comisión también examinará las listas que figuran en los anexos II y III, así como la coherencia en la identificación de los operadores de servicios esenciales y de los servicios en los sectores que figuran en el anexo II. El primer informe se presentará a más tardar tres años después del … [*57 meses después de la entrada en vigor de la presente Directiva*].

Artículo 24

Medidas transitorias

1. Sin perjuicio del artículo 25 y con el fin de ofrecer a los Estados miembros oportunidades adicionales de cooperación durante el plazo de transposición, el Grupo de cooperación y la red de CSIRT empezarán a ejercer las funciones que se establecen en los artículos 11 apartado 3, y 12, apartado 3, respectivamente, a más tardar el … [*seis meses después de la entrada en vigor de la presente Directiva*].

2. En el periodo comprendido entre el… [*seis meses después de la entrada en vigor de la presente Directiva*] y el …[*veintisiete meses después de la entrada en vigor de la presente Directiva*], y a efectos de ayudar a los Estados miembros a adoptar un planteamiento coherente en el proceso de identificación de los operadores de servicios esenciales, el Grupo de cooperación examinará el proceso, el contenido y el tipo de medidas nacionales que permitan la identificación de los operadores de servicios esenciales en un sector específico, de acuerdo con los criterios que figuran en los artículos 5 y 6. A petición de un Estado miembro, el Grupo de cooperación también examinará proyectos específicos nacionales de medidas de dicho Estado miembro, que permitan la identificación de los operadores de servicios esenciales en un sector específico, de acuerdo con los criterios que figuran en los artículos 5 y 6.

3. A más tardar el … [*seis meses después de la entrada en vigor de la presente Directiva*] y a efectos del presente artículo, los Estados miembros harán lo necesario para estar convenientemente representados en el Grupo de cooperación y en la red de CSIRT.

Artículo 25

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar el…[21 meses después de la fecha de entrada en vigor de la presente Directiva], las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Informarán de ello inmediatamente a la Comisión.

Aplicarán esas medidas a partir del … *[día siguiente a la fecha mencionada en el párrafo primero]*.

Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 26

Entrada en vigor

La presente Directiva entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea.*

Artículo 27

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en …, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

ANEXO I

Requisitos y funciones de los equipos de respuesta a incidentes de seguridad informática (CSIRT)

Los requisitos y funciones de los CSIRT se definirán adecuada y claramente y se basarán en la política o la normativa nacional. Incluirán lo siguiente:

(1) Requisitos que deben cumplir los CSIRT

a) Los CSIRT 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) Las dependencias de los CSIRT y los sistemas de información de apoyo estarán situados en lugares seguros.

c) Continuidad de las actividades:

i) Los CSIRT estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.

ii) Los CSIRT contarán con personal suficiente para garantizar su disponibilidad en todo momento.

iii) Los CSIRT dependerán de infraestructuras cuya continuidad esté asegurada. A tal fin, se dispondrá de sistemas redundantes y espacios de trabajo de reserva.

d) Los CSIRT podrán participar, cuando lo deseen, en redes de cooperación internacional.

(2) Funciones de los CSIRT

a) Las funciones de los CSIRT incluirán como mínimo las siguientes:

i) supervisar incidentes a escala nacional,

ii) difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados,

iii) responder a incidentes,

iv) efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación,

v) participar en la red de CSIRT.

b) Los CSIRT establecerán relaciones de cooperación con el sector privado.

c) A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas de:

i) procedimientos de gestión de incidentes y riesgos,

ii) sistemas de clasificación de incidentes, riesgos e información.

ANEXO II

Tipos de entidades a efectos del punto 4 del artículo 4

Sector	Subsector	Tipo de entidad
1. Energía	a) Electricidad	- Empresas eléctricas, tal como se definen en el punto 35 del artículo 2 de la Directiva 2009/72/CE del Parlamento Europeo y del Consejo[1], que efectúa la función de «suministro», tal como se define en el punto 19 del artículo 2 de dicha Directiva
		- Gestores de la red de distribución, tal como se definen en el punto 6 del artículo 2 de la Directiva 2009/72/CE
		Gestores de la red de transporte, tal como se definen en el punto 4 del artículo 2 de la Directiva 2009/72/CE
	b) Crudo	- Operadores de oleoductos de transporte de crudo
		- Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte

[1] Directiva 2009/72/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre normas comunes para el mercado interior de la electricidad y por la que se deroga la Directiva 2003/54/CE (DO L 211 de 14.8.2009, p. 55).

Sector	Subsector	Tipo de entidad
	c) Gas	- Empresas suministradoras, tal como se definen en el punto 8 del artículo 2 de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo[1]
		- Gestores de la red de distribución, tal como se definen en el punto 6 del artículo 2 de la Directiva 2009/73/CE
		- Gestores de la red de transporte, tal como se definen en el punto 4 del artículo 2 de la Directiva 2009/73/CE
		- Gestores de almacenamiento, tal como se definen en el punto 10 del artículo 2 de la Directiva 2009/73/CE
		- Gestores de la red de GNL, tal como se definen en el punto 12 del artículo 2 de la Directiva 2009/73/CE
		- Compañías de gas natural, tal como se definen en el punto 1 del artículo 2 de la Directiva 2009/73/CE
		- Gestores de las instalaciones de refinado y tratamiento de gas natural

[1] Directiva 2009/73/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre normas comunes para el mercado interior del gas natural y por la que se deroga la Directiva 2003/55/CE (DO L 211 de 14.8.2009, p. 94).

Sector	Subsector	Tipo de entidad
2. Transporte	a)Transporte aéreo	- Compañías aéreas, tal como se definen en el punto 4 del artículo 3 del Reglamento (UE) n.º 300/2008 del Parlamento Europeo y del Consejo[1]
		- Entidades gestoras de los aeropuertos, tal como se definen en el punto 2 del artículo 2 de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo[2], aeropuertos, tal como se definen en el punto 1 del artículo 2 de dicha Directiva, incluidos los aeropuertos de la red básica enumerados en la sección 2 del anexo II del Reglamento n.º 1315/2013 del Parlamento Europeo y del Consejo[3], y entidades que gestionan instalaciones auxiliares que comprenden los aeropuertos
		- Operadores de control de la gestión del tráfico que prestan el servicio de control del tránsito aéreo, tal como se definen en el punto 1 del artículo 2 del Reglamento (CE) n.º 549/2004 del Parlamento Europeo y del Consejo[4]

[1] Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002 (DO L 97 de 9.4.2008, p. 72).

[2] Directiva 2009//12/CE del Parlamento Europeo y del Consejo de 11 de marzo de 2009 relativa a las tasas aeroportuarias (DO L 70 de 14.3.2009, p. 11).

[3] Reglamento n.º 1315/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, sobre las orientaciones de la Unión para el desarrollo de la Red Transeuropea de Transporte, y por el que se deroga la Decisión n.º 661/2010/UE (DO L 348 de 20.12.2013, p. 1).

[4] Reglamento (CE) n.º 549/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se fija el marco para la creación del cielo único europeo (Reglamento marco) (DO L 96 de 31.3.2004, p. 1).

Sector	Subsector	Tipo de entidad
	b) Transporte por ferrocarril	- Administradores de infraestructuras, tal como se definen en el punto 2 del artículo 3, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo[1]
		- Empresas ferroviarias, tal como se definen en el punto 1 del artículo 3, de la Directiva 2012/34/UE, incluidos los explotadores de las instalaciones de servicio, tal como se definen en el punto 12 del artículo 3, de la Directiva 2012/34/UE
	c)Transporte marítimo y fluvial	- Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros y como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo[2], sin incluir los buques particulares explotados por esas empresas
		- Organismos gestores de los puertos, tal como se definen en el punto 1 del artículo 3 de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo[3], incluidas sus instalaciones portuarias, tal como se definen en el punto 11 del artículo 2 del Reglamento (CE) n.º 725/2004 y las entidades que operan con las obras y equipos que se encuentran en los puertos

[1] Directiva 2012/34/UE del Parlamento Europeo y del Consejo, de 21 de noviembre de 2012, por la que se establece un espacio ferroviario europeo único (DO L 343 de 14.12.2012, p. 32).

[2] Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias (DO L 129 de 29.4.2004, p. 6).

[3] Directiva 2005/65/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, sobre mejora de la protección portuaria (DO L 310 de 25.11.2005, p. 28).

Sector	Subsector	Tipo de entidad
		- Operadores de servicios de tráfico de buques, tal como se definen en la letra o) del artículo 3 de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo[1]
	d) Transporte por carretera	- Autoridades viarias, tal como se definen en el punto 12 del artículo 2 del Reglamento Delegado (UE) 2015/962 de la Comisión[2], responsables del control de la gestión del tráfico
		- Operadores de los sistemas de transporte inteligentes, tal como se definen en el punto 1 del artículo 4 de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo[3]
3. Banca		Entidades de crédito, tal como se definen en el punto 1 del artículo 4 del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo[4]

[1] Directiva 2002/59/CE del Parlamento Europeo y del Consejo, de 27 de junio de 2002, relativa al establecimiento de un sistema comunitario de seguimiento y de información sobre el tráfico marítimo y por la que se deroga la Directiva 93/75/CEE del Consejo (DO L 208 de 5.8.2002, p. 10).

[2] Reglamento Delegado (UE) 2015/962 de la Comisión de 18 de diciembre de 2014 por el que se complementa la Directiva 2010/40/UE del Parlamento Europeo y del Consejo en lo que se refiere al suministro de servicios de información de tráfico en tiempo real en toda la Unión Europea (DO L 157 de 23.6.2015, p. 21).

[3] Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte (DO L 207 de 6.8.2010, p. 1).

[4] Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y empresas de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013 p. 1).

Sector	Subsector	Tipo de entidad
4. Infraestructuras de los mercados financieros		- Gestores de centros de negociación, tal como se definen en el punto 24 del artículo 4 de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo[1]
		- Entidades de contrapartida central (CCP), tal como se definen en el punto 1 del artículo 2 del Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo[2]
5. Sector sanitario	Entornos de asistencia sanitaria (entre ellos hospitales y clínicas privadas)	Prestadores de asistencia sanitaria, tal como se definen en la letra g) del artículo 3 de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo[3]
6. Suministro y distribución de agua potable		Suministradores y distribuidores de aguas destinadas al consumo humano, tal como se definen en el punto 1, letra a), del artículo 2 de la Directiva 98/83/CE[4], pero sin incluir a los distribuidores para los que la distribución de aguas destinadas al consumo humano constituye solo una parte de su actividad general de distribución de otros bienes y productos básicos que no se consideran servicios esenciales.
7. Infraestructura digital		- IXP
		- Proveedores de servicios del DNS
		- Registros de nombres de dominio de primer nivel

[1] Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349).

[2] Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones (DO L 201 de 27.7.2012, p. 1).

[3] Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

[4] Directiva 98/83/CE del Consejo, de 3 de noviembre de 1998, relativa a la calidad de las aguas destinadas al consumo humano (DO L 330 de 5.12.1998, p. 32).

ANEXO III

Tipos de servicios digitales a efectos del punto 5 del artículo 4

1. Mercado en línea

2. Motor de búsqueda en línea

3. Servicios de computación en nube