Consejo de la Unión Europea

Bruselas, 26 de noviembre de 2021
(OR. en)

14337/21

Expediente interinstitucional: 2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTA

De:	Secretaría General del Consejo
A:	Consejo
N.º doc. prec.:	9583/2/21, 11724/21
N.° doc. Ción.:	14150/20
Asunto:	Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva 2016/1148 *- Orientación general*

I. INTRODUCCIÓN

1. El 16 de diciembre de 2020, la Comisión adoptó la propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad («Directiva SRI revisada» o «Directiva SRI 2»)[1] con el objetivo de sustituir la actual Directiva sobre la seguridad de las redes y sistemas de información («Directiva SRI»)[2].

[1] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148.

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

La propuesta era una de las acciones previstas en la Estrategia de Ciberseguridad de la UE para la Década Digital[3] al objeto de garantizar que los ciudadanos y las empresas puedan disponer de tecnologías digitales fiables.

2. La propuesta está basada en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE) y tiene como finalidad seguir mejorando la resiliencia y las capacidades de respuesta ante incidentes de las entidades públicas y privadas, las autoridades competentes y la Unión en su conjunto.

3. En el Parlamento Europeo, la comisión competente para la propuesta es la Comisión de Industria, Investigación y Energía (ITRE). La Comisión ITRE aprobó el informe del ponente el 28 de octubre de 2021.

4. El Comité Económico y Social Europeo adoptó su dictamen el 28 de abril de 2021.

5. El 3 de febrero de 2021, el Comité de Representantes Permanentes decidió consultar al Comité Europeo de las Regiones sobre la propuesta[4]. Hasta la fecha, el Comité Europeo de las Regiones no ha emitido su dictamen.

6. El Supervisor Europeo de Protección de Datos aprobó su dictamen el 11 de marzo de 2021[5].

7. En sus Conclusiones[6] de 22 de marzo de 2021 sobre la Estrategia de Ciberseguridad de la UE para la Década Digital, el Consejo tomó nota de la nueva propuesta, que está basada en la Directiva SRI, y reiteró su apoyo al refuerzo y la armonización de los marcos nacionales de ciberseguridad y a la cooperación continua entre los Estados miembros.

8. En sus Conclusiones de los días 21 y 22 de octubre de 2021, el Consejo Europeo pidió que se impulsaran los trabajos sobre la propuesta de revisión de la Directiva SRI.

---

3 14133/20.
4 5573/21.
5 Dictamen 5/2021 sobre la Estrategia de Ciberseguridad y la Directiva SRI 2.0.
6 6722/21.

II. TRABAJOS EN LOS ÓRGANOS PREPARATORIOS DEL CONSEJO

9. En el Consejo, fue el Grupo Horizontal «Cuestiones Cibernéticas» el órgano encargado de estudiar la propuesta (en lo sucesivo, Grupo «Ciber»). El estudio de la propuesta comenzó el 19 de enero, durante la Presidencia portuguesa, con una minuciosa lectura que permitió que los Estados miembros formularan sus preguntas, expusieran sus principales preocupaciones y recibieran explicaciones detalladas de la Comisión sobre los cambios introducidos en la Directiva revisada.

10. Durante la Presidencia portuguesa, el Grupo Horizontal dedicó diecisiete reuniones a la presentación y lectura de la propuesta. El 4 de junio de 2021 se presentó al Consejo de Transporte, Telecomunicaciones y Energía un informe de situación de dicha lectura.

11. Desde entonces, los trabajos han proseguido y se han intensificado durante la Presidencia eslovena, al objeto de alcanzar una orientación general en la reunión del Consejo de Transporte, Telecomunicaciones y Energía del 3 de diciembre de 2021. La Presidencia eslovena dedicó quince reuniones a la revisión de la propuesta SRI 2 y numerosos debates bilaterales en todos los niveles.

12. El Grupo «Ciber» centró sus trabajos en modificar la redacción del texto de la propuesta, en primer lugar en lo relativo a la interacción entre la Directiva SRI 2 y la legislación y ámbito de aplicación sectoriales —en particular con respecto a la administración pública, los servidores raíz de DNS y la cláusula de exclusión— y después, entre otros temas, en lo relativo a las revisiones interpares, la jurisdicción y la asistencia mutua, la divulgación coordinada de vulnerabilidades, las bases de datos de nombres de dominio y datos de registro y la cooperación internacional.

13. El 21 de septiembre de 2021 se presentó una primera propuesta transaccional sobre el texto de la Directiva propuesta[7] a partir de los comentarios escritos y documentos oficiosos transmitidos por los Estados miembros, así como de las propuestas transaccionales previas sobre la interacción de la Directiva SRI 2 con la legislación y el ámbito de aplicación sectoriales de la Directiva SRI 2.

---

7 12019/21.

14. La última revisión[8] de la propuesta transaccional de la Presidencia se debatió en el Grupo el 22 de noviembre de 2021. Si bien, en general, las delegaciones acogieron favorablemente el texto transaccional, algunas de ellas aún formularon reservas de estudio u observaciones sobre determinadas partes de la propuesta transaccional. Se sugirieron además algunos cambios técnicos en la redacción de ciertas partes del texto.

III. ELEMENTOS PRINCIPALES

15. A partir de los debates habidos en el Grupo, se ha determinado que las principales cuestiones políticas son las siguientes:

a) Ámbito de aplicación (artículo 2)

Desde el inicio de los debates sobre la propuesta SRI 2, la principal preocupación expresada por los Estados miembros ha sido el aumento considerable del número de entidades que cubre la Directiva y, en particular, la introducción de la norma sobre el tamaño máximo, según la cual todas las entidades medianas y grandes que operen en sectores o presten servicios cubiertos por la Directiva SRI 2 entran en el ámbito de aplicación de esta. Si bien la propuesta transaccional mantiene esta regla general, también incluye disposiciones adicionales para garantizar la proporcionalidad necesaria, un nivel más elevado de gestión de riesgos y unos criterios claros de criticidad para determinar las entidades que entran en el ámbito de aplicación de la Directiva. Además, la propuesta transaccional incluye disposiciones específicas sobre la aplicación prioritaria de las medidas de supervisión con arreglo a un planteamiento basado en los riesgos.

[8] 12019/5/21 REV 5

b) Administración pública (artículo 2, apartado 2 *bis*)

La inclusión de la administración pública en el ámbito de aplicación de la Directiva SRI 2 ha sido un tema muy debatido, dado que este sector es más específico que otros sectores cubiertos por esta. La Presidencia ha buscado un enfoque equilibrado que tuviera en cuenta las especificidades de los marcos nacionales de la administración pública y garantizara a los Estados miembros cierto grado de flexibilidad a la hora de determinar las entidades de la administración pública que entran en el ámbito de aplicación de la Directiva. Por lo tanto, en el texto transaccional, la Directiva SRI 2 se aplica a las entidades de la administración pública de los gobiernos centrales, pero los Estados miembros también pueden disponer que se aplique a las entidades de la administración pública de nivel regional y local.

c) Cláusula de exclusión [artículo 2, apartados 3 *bis* y 3 *bis bis*]

Los Estados miembros deseaban aclarar en mayor medida la cláusula de exclusión, en el sentido de que la Directiva no se aplica a las entidades que realizan actividades principalmente en los ámbitos de la defensa, la seguridad nacional, la seguridad pública o la policía, ni a las actividades relacionadas con la seguridad o la defensa nacionales. También quedan excluidos el poder judicial, los parlamentos y los bancos centrales.

d) Interacción con la legislación sectorial

Los Estados miembros han subrayado la necesidad de armonizar la Directiva SRI 2 con la legislación sectorial, en particular con el Reglamento sobre la resiliencia operativa digital del sector financiero y la Directiva sobre la resiliencia de las entidades críticas. La Directiva SRI 2, que debe ser el referente para la armonización mínima en materia de ciberseguridad, contiene un artículo específico sobre los actos de la Unión sectoriales (artículo 2 *ter*). Por lo que se refiere a la interacción con la Directiva sobre la resiliencia de las entidades críticas, la propuesta transaccional garantiza una mayor claridad en cuanto al planteamiento que abarca todos los peligros. Otras adiciones importantes conciernen los acuerdos de cooperación entre autoridades competentes en virtud de los actos jurídicos correspondientes.

e) Aprendizaje entre iguales (artículo 16)

Con algunas excepciones, los Estados miembros se oponían a que la Comisión estableciera revisiones entre iguales obligatorias. La solución transaccional propuesta garantiza que el nuevo mecanismo de aprendizaje entre iguales esté basado en la confianza mutua y sea un proceso voluntario impulsado por los Estados miembros.

f) Jurisdicción y territorialidad (artículo 24) y asistencia mutua (artículo 34)

Los Estados miembros han expresado su preocupación por las consecuencias que implica dotarse de una jurisdicción diferenciada para las entidades del sector de las TIC, tal como propone la Comisión. El texto transaccional aclara la jurisdicción en función del tipo de entidades y mejora la redacción sobre la asistencia mutua.

g) Obligaciones de información (artículo 20)

A raíz de la preocupación expresada por los Estados miembros de que la obligación de informar sobre amenazas cibernéticas manifiestas hiciera recaer sobre las entidades cubiertas por la Directiva SRI 2 una carga excesiva y provocara un número ingente de notificaciones, en el texto transaccional se ha eliminado dicha obligación.

IV. CONCLUSIÓN

16. El 24 de noviembre de 2021, el Comité de Representantes Permanentes alcanzó un acuerdo sobre el texto transaccional que se adjunta en anexo y decidió presentarlo al Consejo de Transporte, Telecomunicaciones y Energía para que este adopte una orientación general.

17. Por consiguiente, se ruega al Consejo que apruebe el texto transaccional presentado por la Presidencia que figura en el anexo y que adopte una orientación general en su sesión del 3 de diciembre de 2021.

ANEXO

Propuesta de

DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148

(Texto pertinente a efectos del EEE)

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[9],

Visto el dictamen del Comité de las Regiones[10],

De conformidad con el procedimiento legislativo ordinario,

[9] DO C [...] de […], p. […].
[10] DO C [...] de […], p. […].

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[11] era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para las redes y los sistemas de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes de ciberseguridad, contribuyendo así al funcionamiento eficaz de la economía y la sociedad de la Unión.

(2) Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han realizado considerables progresos en el incremento del nivel de resiliencia en materia de ciberseguridad de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y reglamentario relativo a la ciberseguridad en la Unión, preparando el camino para un cambio significativo de mentalidad. Con ella se ha logrado la realización de marcos nacionales mediante la definición de estrategias nacionales […] **sobre seguridad de las redes y de los sistemas de información**, el establecimiento de las capacidades nacionales y la aplicación de medidas reglamentarias que abarcan a los actores y las infraestructuras esenciales identificados por cada Estado miembro. Asimismo, ha propiciado la cooperación a escala de la Unión mediante el establecimiento del Grupo de Cooperación[12] y de **la** […] red de equipos de respuesta a incidentes de seguridad informática («Red de CSIRT»)[13]. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes que impiden un abordaje eficaz de los retos contemporáneos y emergentes en el ámbito de la ciberseguridad.

---

11 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

12 Artículo 11 de la Directiva (UE) 2016/1148.

13 Artículo 12 de la Directiva (UE) 2016/1148.

(3) Las redes y los sistemas de información se han convertido en un aspecto indispensable del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad, también en los intercambios transfronterizos. Esta evolución ha causado una expansión del panorama de amenazas de ciberseguridad, con la consiguiente aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes de ciberseguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y los sistemas de información. Como consecuencia de ello, los incidentes cibernéticos pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, menoscabar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión. Por consiguiente, la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca para que el mercado interior funcione correctamente.

(4) La base jurídica de la Directiva (UE) 1148/2016 era el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), cuyo objetivo es el establecimiento y el funcionamiento del mercado interior mediante el refuerzo de las medidas destinadas a la aproximación de las normas nacionales. Los requisitos de ciberseguridad que se imponen a las entidades que prestan servicios o actividades pertinentes desde el punto de vista económico varían considerablemente en función del Estado miembro por lo que respecta al tipo de requisito, su nivel de detalle y el método de supervisión. Estas disparidades conllevan costes adicionales y generan dificultades para las empresas que ofrecen productos o servicios transfronterizos. Los requisitos impuestos por un Estado miembro que difieren de los aplicados por otro Estado miembro, o incluso los contradicen, pueden afectar sustancialmente a las mencionadas actividades transfronterizas.

Además, es probable que una concepción o una aplicación subóptimas de las **medidas** […] de ciberseguridad en un Estado miembro tenga repercusiones para el nivel de ciberseguridad de otros Estados miembros, especialmente habida cuenta de la intensidad de los intercambios transfronterizos. La revisión de la Directiva (UE) 2016/1148 ha demostrado la existencia de grandes diferencias en su aplicación por parte de los Estados miembros, en particular por lo que respecta a su ámbito de aplicación, cuya delimitación se dejó en gran medida a discreción de los Estados miembros. Asimismo, la Directiva (UE) 2016/1148 confería a los Estados miembros una discrecionalidad muy amplia en lo tocante a la aplicación de las obligaciones de seguridad y notificación de incidentes en ella establecidas. En consecuencia, dichas obligaciones se aplicaron de maneras considerablemente diferentes a escala nacional. Se observaron diferencias similares en la aplicación de las disposiciones relativas a la supervisión y la ejecución de la Directiva.

(5) Todas esas diferencias conllevan una fragmentación del mercado interior y pueden tener un efecto perjudicial para su funcionamiento, afectando, en particular, a la prestación transfronteriza de servicios y al nivel de resiliencia en el ámbito de la ciberseguridad debido a la aplicación de […] **medidas** diferentes. El objetivo de la presente Directiva es eliminar estas divergencias tan pronunciadas entre los Estados miembros, concretamente mediante el establecimiento de las normas mínimas relativas al funcionamiento de un marco reglamentario coordinado, la fijación de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera efectiva, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la facilitación de vías de recurso y sanciones eficaces que son fundamentales para garantizar el cumplimiento efectivo de dichas obligaciones. Por consiguiente, procede derogar la Directiva (UE) 2016/1148 y sustituirla por la presente Directiva.

(6) […] Los Estados miembros **han de poder** adoptar las medidas necesarias para garantizar la protección de los intereses esenciales para su seguridad, preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales […]. […] **La Directiva no debe aplicarse a determinadas entidades públicas o privadas que desempeñen actividades en estos ámbitos**. **Tampoco debe aplicarse a las actividades de entidades que se desempeñen en estos ámbitos. Además,** ningún Estado miembro ha de estar obligado a facilitar información cuya divulgación sea contraria a los intereses esenciales de su seguridad pública. […] **L**as normas nacionales **o** […] de la Unión en materia de protección de la información clasificada, los acuerdos sobre confidencialidad y los acuerdos de confidencialidad informales como el Protocolo TLP para el intercambio de información[14].

(6 *bis*) En virtud de la presente Directiva, el Derecho de la Unión en materia de protección de datos personales y de la intimidad se aplica a todo tratamiento de datos personales. En particular, la presente Directiva se entiende sin perjuicio del Reglamento (UE) 2016/679 y de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo y, por lo tanto, no debe afectar, en particular, a las funciones y facultades de las autoridades de control independientes competentes para supervisar el cumplimiento de la legislación pertinente de la Unión en materia de protección de datos.

---

14 El Protocolo TLP para el intercambio de información es un medio que permite a todo aquel que comparta información comunicar a los destinatarios las posibles limitaciones a la divulgación ulterior de dicha información. Se utiliza en prácticamente todas las comunidades de CSIRT y en algunos Centros de puesta en común y análisis de la información.

(7) Con la derogación de la Directiva (UE) 2016/1148, es preciso hacer extensivo el ámbito de aplicación por sectores a una parte mayor de la economía, habida cuenta de las consideraciones expuestas en los considerandos 4 a 6. En consecuencia, los sectores amparados por la Directiva (UE) 2016/1148 deben ampliarse para ofrecer una cobertura global de los sectores y servicios de vital importancia para las actividades sociales y económicas fundamentales dentro del mercado interior. Las normas no deben ser diferentes según las entidades sean operadores de servicios esenciales o proveedores de servicios digitales. Dicha diferenciación ha quedado obsoleta, ya que no refleja la importancia real de los sectores o servicios para las actividades sociales y económicas en el mercado interior.

(8) Con arreglo a lo dispuesto en la Directiva (UE) 2016/1148, los Estados miembros eran responsables de determinar qué entidades cumplían los criterios para que se considerasen operadores de servicios esenciales («proceso de identificación»). A fin de eliminar las profundas divergencias entre los Estados miembros en ese sentido y garantizar seguridad jurídica para todas las entidades pertinentes respecto a los requisitos de gestión del riesgo y las obligaciones de notificación, debe establecerse un criterio uniforme que determine las entidades que están incluidas en el ámbito de aplicación de la presente Directiva. Dicho criterio debe consistir en la aplicación de la norma sobre el tamaño máximo, por la que todas las empresas medianas y grandes, conforme a la definición recogida en la Recomendación 2003/361/CE[15] de la Comisión, que operen en los sectores o presten el tipo de servicios amparados por la presente Directiva queden incluidos en su ámbito de aplicación. […]

[15] 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).

(8 *bis*) A fin de obtener una perspectiva clara de las entidades incluidas en el ámbito de aplicación de la presente Directiva, los Estados miembros deben poder establecer mecanismos nacionales de autonotificación que obliguen a las entidades a las que se aplica la presente Directiva a comunicar a las autoridades competentes en virtud de la presente Directiva o a los organismos designados a tal fin por los Estados miembros al menos su nombre, dirección y datos de contacto, así como el sector en el que operan o el tipo de servicio que prestan y, cuando proceda, una lista de los Estados miembros en los que la entidad presta sus servicios,. Los Estados miembros podrán decidir sobre los mecanismos adecuados cuando existan a escala nacional registros que permitan identificar a las entidades incluidas en el ámbito de aplicación de la presente Directiva.

(9) […] **L**a presente Directiva también debe ser aplicable a las microentidades o pequeñas entidades que cumplan determinados criterios que indiquen que desempeñan un papel clave para las economías o las sociedades de los Estados miembros, o en el caso de sectores o tipos de servicios concretos. Los Estados miembros deben encargarse de […] presentar […] a la Comisión […] **información pertinente sobre, al menos, el número de entidades determinadas, el sector al que pertenecen o el tipo de servicio que prestan, y los criterios específicos en los que se basan. Los Estados miembros también pueden decidir presentar a la Comisión, cuando ello sea conforme a las normas nacionales de seguridad, los nombres de dichas entidades.**

(9 *bis*) Quedan excluidas del ámbito de aplicación de la presente Directiva las entidades de la administración pública que realicen actividades en los ámbitos de la seguridad nacional, la defensa, la seguridad pública, la policía, así como el poder judicial, los parlamentos y los bancos centrales. A los efectos de la presente Directiva, se considera que las entidades con competencia reguladora no realizan actividades en el ámbito policial y, por lo tanto, no quedan excluidas por ese motivo del ámbito de aplicación de la presente Directiva. Por otra parte, no entran en el ámbito de aplicación de la presente Directiva las entidades de la administración pública del gobierno central establecidas conjuntamente con un tercer país en virtud de un acuerdo internacional.

(9 *bis bis*) Los Estados miembros han de poder establecer que las entidades que antes de la entrada en vigor de la presente Directiva se consideraran operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 deben considerarse entidades esenciales.

(9 *bis bis bis*) La presente Directiva no se aplicará a las misiones diplomáticas y consulares de los Estados miembros en el extranjero ni a sus infraestructuras de TIC que utilicen dichas misiones, en la medida en que estas infraestructuras estén situadas en el extranjero o sean explotadas para usuarios en el extranjero.

(10) La Comisión, en cooperación con el Grupo de Cooperación, puede publicar directrices sobre la aplicación de los criterios aplicables a las microempresas y pequeñas empresas.

(11) […] **Las entidades incluidas en el ámbito de aplicación de la presente Directiva se clasificarán en dos categorías: las esenciales e importantes en función del grado de importancia del sector, o del tipo de servicios que presten y de su tamaño. A este respecto, también deben tenerse debidamente en cuenta las evaluaciones de riesgos sectoriales pertinentes o las orientaciones de las autoridades competentes, cuando proceda.** Las entidades esenciales e importantes han de estar sujetas a […] requisitos de gestión del riesgo y a […] obligaciones de notificación. Los regímenes de supervisión y de sanciones deben ser diferentes para las dos categorías de entidades, a fin de garantizar un equilibrio justo entre los requisitos **en función del riesgo** y las obligaciones, por un lado, y la carga administrativa derivada de la supervisión del cumplimiento, por el otro.

(12) **La presente Directiva constituye la base de referencia para las medidas de gestión de riesgos de ciberseguridad y las obligaciones de notificación en todos los sectores incluidos en su ámbito de aplicación. A fin de evitar la fragmentación de las disposiciones en materia de ciberseguridad de los actos jurídicos de la Unión, cuando se consideren necesarias disposiciones sectoriales adicionales sobre las** medidas de gestión de riesgos en materia de ciberseguridad **y las obligaciones de información para garantizar un elevado nivel de ciberseguridad, la Comisión habrá de evaluar si tales disposiciones podrían establecerse en un acto de ejecución en virtud de la habilitación prevista en la presente Directiva. En caso de que este tipo de acto no correspondiera al objetivo,** la legislación y los instrumentos sectoriales **podrían** contribuir a garantizar **un** nivel[…] elevado[…] de ciberseguridad, teniendo al mismo tiempo plenamente en cuenta las especificidades y complejidades de […] **los** sectores **de que se trate**. **El razonamiento según el cual un acto de ejecución en virtud de la habilitación prevista en la presente Directiva no es adecuado habrá de explicarse en la legislación sectorial específica. Al mismo tiempo, dichas disposiciones sectoriales de los actos jurídicos de la Unión han de tener debidamente en cuenta la necesidad de un marco de ciberseguridad general y armonizado.** […] Ello […] debe entenderse sin perjuicio de las competencias de ejecución existentes que se han conferido a la Comisión en varios sectores, como, por ejemplo, el del transporte y la energía.

(12 *bis*) Cuando un acto de la Unión de carácter sectorial **incluya disposiciones** que exija**n** a las entidades esenciales o importantes adoptar **medidas que tengan un efecto al menos equivalente al de las obligaciones establecidas en la presente Directiva en relación con** la gestión del riesgo de ciberseguridad […] y la obligación de notificar los incidentes **significativos** o las ciberamenazas significativas […], dichas disposiciones sectoriales, **en particular las relativas a la supervisión y la ejecución**, deben aplicarse. **Al determinar el efecto equivalente de las obligaciones establecidas en las disposiciones sectoriales de un acto jurídico de la Unión, deben tenerse en cuenta los siguientes aspectos: i) las medidas de gestión de los riesgos de ciberseguridad deben consistir en medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos relativos a la seguridad de las redes y los sistemas de información que las entidades pertinentes utilizan para prestar sus servicios, y deben incluir como mínimo todos los elementos establecidos en la presente Directiva; ii) la obligación de notificar los incidentes y ciberamenazas significativos debe ser al menos equivalente a las obligaciones establecidas en la presente Directiva con respecto al contenido, el formato y los plazos de las notificaciones; iii) las modalidades de notificación por las entidades y autoridades pertinentes establecidas en los actos jurídicos sectoriales de la Unión deben ser al menos equivalentes a los requisitos establecidos en la presente Directiva con respecto a su contenido, formato y plazos, y deben tener en cuenta el papel de los CSIRT; iv) los requisitos de cooperación transfronteriza para las autoridades pertinentes deben ser al menos equivalentes a los establecidos en la presente Directiva. Si las disposiciones sectoriales de un acto jurídico de la Unión no abarcan a todas las entidades de un sector específico que entre en el ámbito de aplicación de la presente Directiva, las disposiciones pertinentes de la presente Directiva deben seguir aplicándose a las entidades no cubiertas por dichas disposiciones sectoriales.**

(12 *bis bis*) La Comisión **debe revisar periódicamente el cumplimiento de la exigencia de efecto equivalente en relación con las disposiciones sectoriales de los actos jurídicos de la Unión** […]. **La Comisión debe consultar al Grupo de Cooperación al preparar la revisión periódica.**

(12 *bis bis bis*) Los futuros actos jurídicos sectoriales de la Unión deben tener debidamente en cuenta las definiciones que figuran en el artículo 4 de la presente Directiva y el marco de supervisión y ejecución establecido en el capítulo VI de la presente Directiva.

(12 *bis ter*) Cuando las disposiciones sectoriales de los actos jurídicos de la Unión exijan a entidades esenciales o importantes que adopten medidas de efecto al menos equivalente a las obligaciones de notificación establecidas en la presente Directiva, debe evitarse la duplicación de las obligaciones de notificación y garantizarse la coherencia y la eficacia de la gestión de las notificaciones de ciberamenazas o incidentes. A tal fin, esas disposiciones sectoriales pueden permitir que los Estados miembros establezcan un mecanismo común, automático y directo de notificación de incidentes y ciberamenazas significativos tanto a las autoridades cuyas tareas se establecen en las disposiciones sectoriales respectivas como a las autoridades competentes, incluido el punto de contacto único y los CSIRT, según proceda, responsables de las tareas de ciberseguridad previstas en la presente Directiva, o un mecanismo que garantice el intercambio sistemático e inmediato de información y la cooperación entre las autoridades pertinentes y los CSIRT en relación con la tramitación de dichas notificaciones. A efectos de simplificar la notificación y de aplicar el mecanismo común, automático y directo de notificación, los Estados miembros pueden, de conformidad con la legislación sectorial específica, utilizar el punto de entrada única que establezcan de conformidad con el artículo 11, apartado 5 *bis*, de la presente Directiva. Para garantizar la armonización, las obligaciones de notificación de los actos jurídicos sectoriales de la Unión deben armonizarse con las establecidas en la presente Directiva. Los Estados miembros pueden determinar que las autoridades competentes, en virtud de la presente Directiva o los CSIRT nacionales, sean los destinatarios de la notificación, de conformidad con las legislaciones sectoriales específicas.

(13) El Reglamento XXXX/XXXX del Parlamento Europeo y del Consejo debe considerarse un acto jurídico de la Unión de carácter sectorial en relación con la presente Directiva por lo que respecta a las entidades del sector financiero. En lugar de las disposiciones **establecidas** […] en la presente Directiva, deben aplicarse las disposiciones del Reglamento XXXX/XXXX relativas a las medidas de gestión de los riesgos de las tecnologías de la información y de las comunicaciones (TIC), a la gestión de los incidentes asociados a las TIC, en particular la notificación de los mismos, así como a las pruebas de la resiliencia operativa digital, los mecanismos de intercambio de información y el riesgo de terceros relacionado con las TIC. En consecuencia, los Estados miembros no deben aplicar las disposiciones de la presente Directiva relativas a las obligaciones de gestión de los riesgos de ciberseguridad y de notificación […] y supervisión y ejecución a ninguna entidad financiera cubierta por el Reglamento XXXX/XXXX. Al mismo tiempo, es importante mantener una estrecha relación y el intercambio de información con el sector financiero al amparo de la presente Directiva. Para ello, el Reglamento XXXX/XXXX permite que […] las Autoridades Europeas de Supervisión (AES) para el sector financiero y las autoridades nacionales competentes en virtud del Reglamento XXXX/XXXX participen en los […] trabajos del Grupo de Cooperación e intercambien información y cooperen con los puntos de contacto únicos designados con arreglo a la presente Directiva, […] **así como** con los CSIRT nacionales. Las autoridades competentes en virtud del Reglamento XXXX/XXXX deben transmitir los detalles de los incidentes graves relacionados con las TIC **y las ciberamenazas significativas** también a los puntos de contacto únicos, a las autoridades competentes o a los CSIRT nacionales designados en virtud de la presente Directiva. **Esto puede lograrse mediante la transmisión automática y directa de las notificaciones de incidentes o mediante una plataforma común de notificación.** Además, los Estados miembros deben seguir incluyendo al sector financiero en sus estrategias de ciberseguridad y […] los CSIRT nacionales pueden ocuparse del sector financiero en sus actividades.

(13 *bis*) **A fin de evitar lagunas y duplicaciones entre las obligaciones en materia de ciberseguridad impuestas a las entidades del sector de la aviación a que se refiere el punto 2, letra a), del anexo I, las autoridades nacionales designadas en virtud de los Reglamentos (CE) n.º 300/2008[16] y (UE) 2018/1139[17] del Parlamento Europeo y del Consejo y las autoridades competentes en virtud de la presente Directiva deben cooperar con respecto a la aplicación de las medidas de gestión de riesgos de ciberseguridad y la supervisión de dichas medidas a escala nacional. Las autoridades nacionales designadas en virtud de los Reglamentos (CE) n.º 300/2008 y (UE) 2018/1139 pueden considerar que una entidad que cumple las medidas de gestión de riesgos de ciberseguridad establecidos en la presente Directiva cumple los requisitos establecidos en dichos Reglamentos y los actos delegados y de ejecución pertinentes adoptados en virtud de dichos Reglamentos.**

---

16 **Reglamento (CE) n.° 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.° 2320/2002 (DO L 97 de 9.4.2008, p. 72).**

17 **Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.º 2111/2005 (CE), n.º 1008/2008, (UE) n.º 996/2010, (UE) n.º 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.º 552/2004 y (CE) n.º 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.º 3922/91 del Consejo (DO L 212 de 22.8.2018, p. 1).**

(14) En vista de los vínculos que existen entre la ciberseguridad y la seguridad física de las entidades, debe mantenerse un enfoque coherente entre la Directiva (UE) XXX/XXX del Parlamento Europeo y del Consejo y la presente Directiva. Para ello, los Estados miembros han de velar por que las entidades críticas, **[**y las entidades equivalentes**]** con arreglo a lo dispuesto en la Directiva (UE) XXX/XXX, se consideren entidades esenciales a los efectos de la presente Directiva. Asimismo, los Estados miembros deben asegurarse de que sus estrategias de ciberseguridad prevean un marco de actuación para una coordinación reforzada entre las autoridades competentes con arreglo a la presente Directiva y las competentes en virtud de la Directiva (UE) XXX/XXX en el contexto del intercambio de información sobre incidentes y ciberamenazas y el ejercicio de las tareas de supervisión. Las autoridades competentes en virtud de ambas Directivas deben cooperar e intercambiar información, en particular en relación con la identificación de las entidades críticas, las ciberamenazas, los riesgos de ciberseguridad y los incidentes, **así como los riesgos, amenazas e incidentes no cibernéticos**, que afecten a las entidades críticas, **[**o a **las entidades equivalentes a entidades críticas]** […], así como en relación con las medidas de ciberseguridad **y físicas** adoptadas por las entidades críticas **y los resultados de las actividades de supervisión realizadas con respecto a dichas entidades**. **Por otra parte, con el fin de racionalizar las actividades de supervisión entre las autoridades competentes designadas en virtud de ambas Directivas y de reducir al mínimo la carga administrativa para las entidades afectadas, las autoridades competentes deben esforzarse por armonizar los modelos de notificación de incidentes y los procesos de supervisión.** […] **Cuando proceda**, las autoridades competentes en virtud de la Directiva (EU) XXX/XXX […] **pueden solicitar** a las autoridades competentes en virtud de la presente Directiva […] que ejerzan sus facultades de supervisión y ejecución […] con respecto a una entidad esencial considerada como crítica. […]

(14 *bis*) Las entidades pertenecientes al sector de las infraestructuras digitales se basan esencialmente en redes y sistemas de información, por lo que las obligaciones impuestas a dichas entidades en virtud de la presente Directiva deben abordar de manera exhaustiva la seguridad física de dichos sistemas como parte de sus obligaciones en materia de gestión de riesgos de ciberseguridad y notificación. Dado que estas cuestiones entran en el ámbito de aplicación de la presente Directiva, las obligaciones establecidas en los capítulos III a VI de la Directiva (UE) XXX/XXX [REC] no se aplican a dichas entidades.

(15) El mantenimiento y la conservación de un sistema de nombres de dominio (DNS) fiable, resiliente y seguro son factores clave para garantizar la integridad de internet y resultan fundamentales para que funcione con estabilidad y de manera ininterrumpida, de lo que depende la economía digital y la sociedad. Por consiguiente, la presente Directiva debe aplicarse a los proveedores de servicios de DNS a lo largo de la cadena de **suministro y** resolución de DNS **que sean importantes para el mercado interior**, incluidos […] los **registros** de nombres de dominio de primer nivel […], **las entidades proveedoras de servicios registro de nombres de dominio, los operadores de** servidores de nombres autoritativos para nombres de dominio y **los operadores de** solucionadores recursivos. **El término «proveedor de servicios de DNS» no debe aplicarse a los servicios de DNS prestados para los propios fines de la entidad de que se trate y sus entidades afiliadas. Las obligaciones en materia de ciberseguridad derivadas de la presente Directiva para esta categoría de proveedores se limitan estrictamente a las medidas de gestión del riesgo de ciberseguridad y a la notificación y, por lo tanto, se entienden sin perjuicio de la gobernanza del DNS mundial por parte de la comunidad multilateral.**

(16) Los servicios de computación en nube deben abarcar los servicios que permiten un acceso remoto bajo demanda y amplio a un conjunto modulable y elástico de recursos informáticos distribuidos que se pueden compartir. Esos recursos informáticos incluyen recursos tales como las redes, los servidores u otras infraestructuras, sistemas operativos, software, almacenamiento, aplicaciones y servicios. **Los modelos de servicios de computación en nube incluyen, entre otros, la infraestructura como servicio (IaaS), la plataforma como servicio (PaaS), el software como servicio (SaaS) y la red como servicio (NaaS).** Los modelos de despliegue de la computación en nube deben abarcar nubes privadas, comunitarias, públicas e híbridas. Los referidos modelos de servicio y despliegue tienen el mismo significado que los términos de los modelos de servicio y despliegue definidos en la norma ISO/IEC 17788:2014. La capacidad del usuario de la computación en nube de autoabastecerse unilateralmente de capacidades de computación, como, por ejemplo, tiempo de servidor o almacenamiento en red, sin ninguna interacción humana por parte del proveedor de servicios de computación en nube podría describirse como administración bajo demanda. La expresión «acceso remoto amplio» se utiliza para describir que las capacidades en la nube se suministran en toda la red y se accede a ellas a través de mecanismos que promueven el uso de plataformas de cliente ligero o pesado heterogéneas (incluidos teléfonos móviles, tabletas, ordenadores portátiles o estaciones de trabajo).

El término «modulable» se refiere a los recursos informáticos 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 el tratamiento se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico. El término «distribuido» se emplea para describir los recursos informáticos que se encuentran ubicados en distintos ordenadores o dispositivos conectados en red y que se comunican y coordinan entre sí intercambiando mensajes.

(17) Habida cuenta de la aparición de tecnologías innovadoras y nuevos modelos de negocio, se espera que surjan en el mercado nuevos modelos de despliegue y servicio de computación en nube en respuesta a la evolución de las necesidades de los clientes. En ese contexto, los servicios de computación en nube pueden prestarse de una forma muy distribuida, más cerca si cabe del punto en que los datos se generan o recogen, abandonando así el modelo tradicional en favor de uno muy distribuido («computación en el borde»)

(18) Los servicios ofrecidos por los proveedores de servicios de centro de datos no siempre pueden prestarse en forma de servicio de computación en nube. En consecuencia, los centros de datos no siempre pueden formar parte de una infraestructura de computación en nube. A fin de gestionar todos los riesgos que se plantean para la seguridad de las redes y sistemas de información, la presente Directiva también debe englobar a los proveedores de estos servicios de centro de datos que no son servicios de computación en nube. A los efectos de la presente Directiva, la expresión «servicio de centro de datos» debe abarcar la prestación de un servicio que englobe las estructuras, o agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de tecnologías de la información y equipos de red que proporcionen servicios de almacenamiento, tratamiento y transporte de datos, junto con todas las instalaciones e infraestructuras destinadas a la distribución de energía y el control ambiental. La expresión «servicio de centro de datos» no se aplica a los centros de datos empresariales internos cuya propiedad y explotación para fines propios dependen de la entidad de que se trate.

(19) Los proveedores de servicios postales en el sentido de la Directiva 97/67/CE del Parlamento Europeo y del Consejo[18], […] **en particular** […] los proveedores de servicios de mensajería, deben estar sujetos a la presente Directiva si se encargan de al menos una de las etapas de la cadena de distribución postal y en particular de la recogida, la clasificación o la distribución, incluida la recogida por el destinatario. Los servicios de transporte que no se lleven a cabo en combinación con alguna de estas etapas deben quedar excluidos del ámbito de los servicios postales.

---

18 Directiva 97/67/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio (DO L 15 de 21.1.1998, p. 14).

(20) Estas crecientes interdependencias obedecen a una red cada vez más transfronteriza e interdependiente de prestaciones de servicios que utilizan infraestructuras clave de toda la Unión en los sectores de la energía, el transporte, la infraestructura digital, el agua potable y las aguas residuales, la sanidad, determinados aspectos de la Administración pública, así como el espacio por lo que respecta a la prestación de determinados servicios que dependen de infraestructuras terrestres cuya propiedad, gestión y explotación residen en los Estados miembros o en entidades privadas, dejando al margen, por tanto, las infraestructuras cuya propiedad, gestión u explotación dependen de la Unión o se efectúan en su nombre como parte de sus programas espaciales. Tales interdependencias implican que cualquier perturbación, incluso aquellas que inicialmente se circunscriben a una entidad o un sector, puede tener efectos en cascada más amplios que pueden dar lugar a impactos con un gran alcance y duración en la prestación de servicios en todo el mercado interior. La pandemia de COVID-19 ha puesto de relieve la vulnerabilidad de nuestras sociedades, cada vez más interdependientes, ante riesgos con probabilidad baja.

(**20 bis**) **Con el fin de lograr y mantener un alto nivel de ciberseguridad, las estrategias nacionales de ciberseguridad exigidas por la presente Directiva deben consistir en marcos coherentes que proporcionen una gobernanza en el ámbito de la ciberseguridad. Estas estrategias pueden constar de uno o varios documentos de carácter legislativo o no.**

(21) 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, los Estados miembros deben poder designar a más de una autoridad nacional competente responsable de ejercer las tareas vinculadas a la seguridad de las redes y los sistemas de información de las entidades esenciales e importantes en virtud de la presente Directiva. Los Estados miembros deben poder asignar esta función a una autoridad existente.

(22) Con el fin de facilitar la cooperación y la comunicación transfronterizas entre las autoridades y de permitir una aplicación efectiva de la presente Directiva, es necesario que cada Estado miembro designe 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.

(23) Las autoridades competentes o los CSIRT deben recibir las notificaciones de incidentes de las entidades de manera eficaz y eficiente, **también con el fin de facilitar, cuando proceda, una respuesta en tiempo oportuno frente a los incidentes, así como una respuesta a la entidad notificante.** Debe encomendarse a los puntos de contacto únicos la transmisión de las notificaciones de incidentes a los puntos de contacto únicos de otros Estados miembros afectados. […]

(23 *bis*) **Los actos jurídicos sectoriales de la Unión que requieran medidas de gestión de riesgos de ciberseguridad u obligaciones de notificación de efecto al menos equivalente al de las establecidas en la presente Directiva podrían establecer que sus autoridades competentes designadas ejerzan sus facultades de supervisión y ejecución relativas a dichas medidas u obligaciones con la ayuda de las autoridades competentes designadas de conformidad con la presente Directiva. Las autoridades competentes pertinentes podrían establecer acuerdos de cooperación a tal fin. Estos acuerdos de cooperación podrían especificar, entre otros elementos, los procedimientos relativos a la coordinación de las actividades de supervisión, en particular los procedimientos para las investigaciones y la inspecciones *in situ* de conformidad con el Derecho nacional y un mecanismo de intercambio de información pertinente entre las autoridades competentes en materia de supervisión y ejecución, que permita también acceder a la información sobre aspectos cibernéticos solicitada por las autoridades competentes designadas de conformidad con la presente Directiva.**

(24) Los Estados miembros deben disponer de capacidades técnicas y de organización adecuadas para poder adoptar medidas de prevención, detección, respuesta y reducción de los incidentes y riesgos que afecten a las redes y sistemas de información. Por tanto, los Estados miembros deben asegurarse de que disponen de CSIRT, también denominados equipos de respuesta a emergencias informáticas (CERT®, por sus siglas en inglés), 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 vistas a reforzar la relación de confianza entre las entidades y los CSIRT, cuando un CSIRT forme parte de una autoridad competente, los Estados miembros […] **pueden** considerar la posibilidad de establecer una separación funcional entre las tareas operativas desempeñadas por los CSIRT, en particular en relación con el intercambio de información y el apoyo prestado a las entidades, y las actividades de supervisión de las autoridades competentes.

(25) Por lo que respecta a los datos personales, los CSIRT deben poder ofrecer, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[19] una exploración proactiva de las redes y los sistemas de información utilizados para la prestación de sus servicios, en nombre de una entidad contemplada por la presente Directiva y a petición de ella. **Cuando proceda**, los Estados miembros deben tratar de garantizar el mismo nivel de capacidades técnicas para todos los CSIRT sectoriales. Los Estados miembros pueden solicitar la asistencia de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) al crear CSIRT nacionales.

(26) 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. **Por consiguiente los CSIRT y las autoridades competentes podrían intercambiar información, incluidos datos personales, con los CSIRT de terceros países o sus autoridades, para el desempeño de sus tareas con arreglo al Reglamento (UE) 2016/679. A falta de una decisión de adecuación adoptada con arreglo al artículo 45 del Reglamento (UE) 2016/679 o de garantías adecuadas con arreglo al artículo 46 de dicho Reglamento, el intercambio de datos personales que se considere necesario para reducir las ciberamenazas significativas y responder a un incidente significativo en curso podría considerarse una razón importante de interés público en el sentido del artículo 49, apartado 1), letra d) del Reglamento 2016/679.**

---

[19] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

(27) De conformidad con al anexo de la Recomendación (UE) 2017/1548 de la Comisión, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (Plan director)[20], por incidente a gran escala debe entenderse un incidente que cause perturbaciones que superen la capacidad de un Estado miembro para responder a él o que afecte significativamente por lo menos a dos Estados miembros. Dependiendo de su causa e impacto, los incidentes a gran escala pueden intensificarse y convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior. Habida cuenta de la amplitud del alcance y, en la mayoría de casos, de la naturaleza transfronteriza de tales incidentes, los Estados miembros y las instituciones, los órganos y los organismos de la Unión pertinentes deben cooperar a nivel técnico, operativo y político para coordinar convenientemente la respuesta en toda la Unión.

(28) Puesto que la explotación de las vulnerabilidades de las redes y sistemas de información puede causar perturbaciones y daños considerables, la determinación y subsanación rápidas de dichas vulnerabilidades son factores importantes para reducir los riesgos de ciberseguridad. En consecuencia, las entidades que desarrollen **o administren** sistemas a tales efectos deben establecer procedimientos apropiados para manejar las vulnerabilidades cuando se detecten. Teniendo en cuenta que las vulnerabilidades suelen ser detectadas y notificadas (reveladas) por terceros (entidades notificantes), los fabricantes o proveedores de productos o servicios de TIC también deben implantar los procedimientos necesarios para recibir información sobre las vulnerabilidades de terceros. En este sentido, las normas internacionales ISO/IEC 30111 e ISO/IEC **29147** ofrecen orientación sobre la gestión de las vulnerabilidades y la divulgación de las vulnerabilidades respectivamente. Por lo que respecta a la divulgación de las vulnerabilidades, la coordinación entre las entidades notificantes y los fabricantes o proveedores de productos o servicios de TIC reviste una gran importancia. La divulgación coordinada de las vulnerabilidades especifica un proceso estructurado a través del cual las vulnerabilidades se notifican a las organizaciones de tal manera que estas puedan diagnosticar y subsanar las vulnerabilidades antes de revelar información detallada sobre ellas a terceros o al público. Asimismo, la divulgación coordinada de las vulnerabilidades debe comprender la coordinación entre la entidad notificante y la organización en lo tocante al momento de la subsanación y la publicación de las vulnerabilidades.

---

20 Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala (DO L 239 de 19.9.2017, p. 36).

(29) Por consiguiente, los Estados miembros deben adoptar medidas para facilitar la divulgación coordinada de las vulnerabilidades mediante el establecimiento de la correspondiente política nacional. **Como parte de su política nacional, los Estados Miembros deben tener como objetivo abordar, en la medida de lo posible, los retos a que se enfrentan los investigadores de vulnerabilidades, en particular la posibilidad de incurrir en responsabilidad penal con arreglo a su ordenamiento jurídico nacional.** […] Los Estados miembros deben designar un CSIRT que asuma el papel de «coordinador» y ejerza de intermediario entre las entidades notificantes y los fabricantes o proveedores de productos o servicios de TIC cuando sea necesario. Las tareas del CSIRT coordinador deben consistir, en particular, en identificar a las entidades afectadas y contactar con ellas, prestar apoyo a las entidades notificantes, negociar los plazos de divulgación y gestionar las vulnerabilidades que afectan a múltiples organizaciones (divulgación **coordinada** de las vulnerabilidades con múltiples interesados). Cuando la vulnerabilidad **notificada pueda afectar de manera significativa a entidades** […] de más de un Estado miembro, los CSIRT designados […] deben cooperar en el marco de la red de CSIRT, **cuando proceda**.

(30) El acceso a información correcta y en tiempo oportuno sobre las vulnerabilidades que afectan a productos y servicios de TIC contribuye a reforzar la gestión de los riesgos de ciberseguridad. En este sentido, las fuentes de información sobre las vulnerabilidades disponibles para el público suponen una herramienta importante para las entidades y sus usuarios, pero también para las autoridades nacionales competentes y los CSIRT. Por este motivo, la ENISA debe crear un registro de vulnerabilidades en el que las entidades esenciales e importantes y sus proveedores, así como las entidades que no estén incluidas en el ámbito de aplicación de la presente Directiva **o los CSIRT designados**, puedan, de manera voluntaria, revelar las vulnerabilidades y facilitar información sobre las mismas que permita a los usuarios adoptar las medidas de mitigación apropiadas.

(31) Aunque efectivamente existen registros o bases de datos de vulnerabilidades similares, su alojamiento y mantenimiento dependen de entidades que no están establecidas en la Unión. Con un Registro Europeo de Vulnerabilidades mantenido por la ENISA se conseguiría mejorar la transparencia del proceso de publicación antes de que la vulnerabilidad se revele oficialmente y la resiliencia en caso de perturbaciones o interrupciones de la prestación de servicios similares. A fin de evitar la duplicación de esfuerzos y lograr la complementariedad en la medida de lo posible, la ENISA debe estudiar la posibilidad de celebrar acuerdos de cooperación estructurada con registros similares en jurisdicciones de terceros países. **Concretamente, ENISA debe estudiar la posibilidad de establecer una cooperación estrecha con los operadores del sistema de Vulnerabilidades y Exposiciones Comunes (CVE por su sigla inglesa), en particular la posibilidad de convertirse en una autoridad de numeración de CVE raíz.**

(32) **El Grupo de Cooperación debe seguir apoyando y facilitando la cooperación estratégica y el intercambio de información, así como seguir reforzando la confianza entre los Estados miembros.** El Grupo de Cooperación debe elaborar cada dos años un programa de trabajo que comprenda las acciones que llevará a cabo para poner en práctica sus objetivos y cometidos. El calendario del primer programa adoptado en virtud de la presente Directiva debe adecuarse al del último programa adoptado con arreglo a la Directiva (UE) 2016/1148 para evitar posibles perturbaciones en el trabajo del Grupo.

(33) A la hora de elaborar documentos de orientación, de manera sistemática el Grupo de Cooperación debe identificar las soluciones y experiencias nacionales, evaluar el impacto de los resultados concretos del Grupo de Cooperación en los enfoques nacionales, debatir los desafíos en materia de aplicación y formular recomendaciones específicas que deben incorporarse mediante la mejora de la aplicación de las normas vigentes.

(34) El Grupo de Cooperación debe seguir siendo un foro flexible y capaz de responder a prioridades y desafíos políticos nuevos y cambiantes, teniendo en cuenta a la vez la disponibilidad de los recursos. Debe organizar reuniones conjuntas periódicas con las partes interesadas privadas pertinentes de toda la Unión para debatir las actividades realizadas por el Grupo y recabar apreciaciones sobre los desafíos políticos emergentes. Con vistas a reforzar la cooperación a escala de la Unión, el Grupo debe considerar la posibilidad de invitar a que participen en sus actividades a los órganos y las agencias de la Unión implicados en la política de ciberseguridad, como por ejemplo el Centro Europeo de Ciberdelincuencia (EC3), la Agencia de la Unión Europea para la Seguridad Aérea (AESA) y la Agencia de la Unión Europea para el Programa Espacial (EUSPA).

(35) Las autoridades competentes y los CSIRT deben estar capacitados para participar en programas de intercambio para funcionarios de otros Estados miembros para mejorar la cooperación. Las autoridades competentes deben adoptar las medidas necesarias para que los funcionarios de otros Estados miembros puedan desempeñar un papel eficaz en las actividades de la autoridad competente de acogida.

(35 *bis*) La Red de CSIRT debe seguir contribuyendo al refuerzo de la confianza y la seguridad y promoviendo una cooperación operativa rápida y eficaz entre los Estados miembros. Con vistas a reforzar la cooperación operativa a escala de la Unión, la Red CSIRT debe considerar la posibilidad de invitar a que participen en sus actividades a los órganos y las agencias de la Unión implicados en la política de ciberseguridad, como por ejemplo la Europol.

(36) […]

(36 *bis*) **A fin de facilitar la aplicación efectiva de las disposiciones de la presente Directiva, como la gestión de las vulnerabilidades, la gestión de los riesgos de ciberseguridad, las medidas de notificación y los mecanismos de intercambio de información, los Estados miembros podrán cooperar con terceros países y emprender actividades que se consideren adecuadas a tal fin, incluidos los intercambios de información sobre las amenazas, los incidentes, las vulnerabilidades, las herramientas y métodos, las tácticas, las técnicas y procedimientos, la preparación y los ejercicios para la gestión de cibercrisis, la formación, el refuerzo de la confianza y los mecanismos estructurados de intercambio de información. Dichos acuerdos de cooperación deben cumplir la legislación de la Unión en materia de protección de datos.**

(37) Los Estados miembros deben contribuir al establecimiento del Marco de respuesta a las crisis de ciberseguridad de la UE recogido en la Recomendación (UE) 2017/1584 a través de las redes de cooperación existentes, en particular la red **europea** de organizaciones de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe), la red de CSIRT y el Grupo de Cooperación. La EU-CyCLONe y la red de CSIRT deben cooperar sobre la base de disposiciones de procedimiento que definan las modalidades de dicha cooperación **y evitar la duplicación de tareas.** El reglamento interno de la EU-CyCLONe debe especificar asimismo las modalidades por las que debe regirse el funcionamiento de la red, incluidos, entre otros, las funciones, los modos de cooperación, las interacciones con otros actores pertinentes y los modelos para el intercambio de información, así como los medios de comunicación. De cara a la gestión de crisis a nivel **político** en la Unión, las partes pertinentes deben recurrir al Dispositivo de la UE de Respuesta Política Integrada a las Crisis (RPIC). La Comisión debe utilizar a tales efectos el proceso de coordinación de crisis intersectoriales de alto nivel ARGUS. Si la crisis tiene una importante dimensión de política exterior o de política común de seguridad y defensa (PCSD), debe activarse el Mecanismo de Respuesta a las Crisis (CRM) del Servicio Europeo de Acción Exterior (SEAE).

(37 *bis*) **La EU-CyCLONe debe servir de red intermediaria entre los niveles técnico y político durante los incidentes y las crisis de seguridad a gran escala. Debe contribuir a mejorar la cooperación a nivel operativo, apoyándose en las constataciones de la red de CSIRT y haciendo uso de sus propias capacidades para realizar una evaluación de impacto de los incidentes y las crisis a gran escala y contribuyendo a la toma de decisiones a nivel político. Las instituciones, órganos y organismos de la UE deben designar a una autoridad competente responsable de la gestión de incidentes y crisis de seguridad a gran escala que sea miembro de la EU-CyCLONe.**

(38) […]

(39) […]

(39 *bis*) **La responsabilidad de velar por la seguridad de las redes y sistemas de información recae en gran medida en las entidades esenciales e importantes. Debe fomentarse y desarrollarse una cultura de gestión de riesgos que implique una evaluación del riesgo y la aplicación de medidas de seguridad adecuadas a los riesgos que se presentan.**

(40) En lo que se refiere a las medidas de gestión del riesgo**, debe tenerse en cuenta el grado de dependencia de la entidad respecto de las redes y los sistemas de información,** y entre ellas deben incluirse medidas cuya finalidad es determinar todo riesgo de incidentes, prevenir, detectar y gestionar incidentes y reducir sus repercusiones. La seguridad de las redes y los sistemas de información debe comprender la seguridad de los datos almacenados, transmitidos y tratados.

(40 *bis*) **Dado que las amenazas para las redes y los sistemas de información pueden originarse por diferentes causas, la presente Directiva aplica un planteamiento que abarca todos los peligros, que incluye la protección de las redes y los sistemas de información y su entorno físico frente a cualquier tipo de suceso, como robos, incendios, inundaciones, fallos en las telecomunicaciones o de suministro de electricidad o frente a cualquier tipo de acceso físico no autorizado o daño a la información que posee la entidad y las instalaciones de procesamiento de información de la entidad, o frente a cualquier tipo de interferencia con dicha información e instalaciones, que puedan comprometer la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. Por tanto, las medidas de gestión de riesgos de ciberseguridad también deben abordar la seguridad física y del entorno, mediante la introducción de medidas orientadas a proteger las redes y los sistemas de información de la entidad frente a los fallos del sistema, errores humanos, acciones malintencionadas o fenómenos naturales, de conformidad con las normas reconocidas a escala europea o internacional, como las que figuran en la serie ISO 27000. A este respecto, las entidades deben abordar asimismo, en el marco de sus medidas de gestión de riesgos de ciberseguridad, la seguridad de los recursos humanos y establecer políticas adecuadas en materia de control del acceso. Esas medidas deben ser coherentes con la Directiva XXXX [Directiva REC].**

(40 *ter*) **A falta de unos esquemas europeos de certificación de la ciberseguridad adecuados y adoptados de conformidad con el Reglamento (UE) 2019/881, los Estados miembros podrían exigir a las entidades, a fin de cumplir los requisitos en materia de gestión de riesgos de ciberseguridad que se establecen en la presente Directiva, que hagan uso de productos, servicios y procesos certificados de TIC u obtener un certificado en virtud de esquemas nacionales de ciberseguridad ya disponibles.**

(41) Para evitar imponer una carga financiera y administrativa desproporcionada a las entidades esenciales e importantes, los requisitos de gestión de los riesgos de ciberseguridad han de ser proporcionados en relación con los riesgos **para** […] la red y el sistema de información en cuestión, teniendo en cuenta el estado de la técnica de esas medidas **y el coste de su aplicación**. **Asimismo debe tenerse debidamente en cuenta el tamaño de la entidad, así como la probabilidad de que se produzcan incidentes y la gravedad de estos.**

(41 *bis*) Para aliviar la carga normativa, los requisitos para la aplicación de las medidas de gestión de riesgos de ciberseguridad para las pequeñas y medianas entidades o microentidades deben ser menos estrictos, a no ser que los criterios sobre el grado de importancia o las evaluaciones de riesgos justificaran la necesidad de unos criterios más estrictos, en particular en lo que respecta a las entidades que cumplan los criterios relacionados con el grado de importancia que se establecen en la presente Directiva.

(42) Las entidades esenciales e importantes deben garantizar la seguridad de las redes y los sistemas de información que utilizan en sus actividades. Se trata fundamentalmente de redes y sistemas de información privados gestionados por el personal informático interno o cuya seguridad se ha encomendado a empresas externas. Los requisitos de gestión de riesgos de ciberseguridad y de notificación en virtud de la presente Directiva deben aplicarse a las entidades esenciales e importantes pertinentes, independientemente de si se encargan ellas mismas del mantenimiento de sus redes y sistemas de información o lo externalizan.

(42 *bis bis*) Teniendo en cuenta su naturaleza transfronteriza, los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados deben estar sujetos a un nivel más elevado de armonización a nivel de la Unión. Por tanto, la aplicación de las medidas de ciberseguridad debe facilitarse por medio de un acto de ejecución.

(43) Hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad y su relación con sus proveedores resulta especialmente importante, habida cuenta de la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y los agentes malintencionados han podido comprometer la seguridad de las redes y los sistemas de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Por ello, las entidades deben evaluar y tener en cuenta la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

(44) Entre los proveedores de servicios, los proveedores de servicios de seguridad administrada en ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría desempeñan un papel especialmente importante al prestar asistencia a las entidades en sus esfuerzos por detectar los incidentes y responder a ellos. No obstante, los propios proveedores de servicios de seguridad administrada también han sido objetivo de ciberataques y plantean un riesgo de ciberseguridad especial como consecuencia de su estrecha integración en los procesos de los operadores. En consecuencia, las entidades deben redoblar su diligencia a la hora de seleccionar un proveedor de servicios de seguridad administrada.

(44 *bis*) Las autoridades nacionales competentes, en el contexto de sus tareas de supervisión, también podrán beneficiarse de los servicios relacionados con la ciberseguridad, como las auditorías de seguridad y las pruebas de penetración o la respuesta a incidentes. Para ayudar a las entidades, así como a las autoridades nacionales competentes, a la hora de seleccionar proveedores de servicios de ciberseguridad cualificados y de confianza, la Comisión, con la ayuda del Grupo de Cooperación y la ENISA, deben considerar la posibilidad de solicitar esquemas europeos de certificación de la ciberseguridad de conformidad con el artículo 48 del Reglamento (UE) 2019/881.

(45) Asimismo, las entidades deben abordar los riesgos de ciberseguridad derivados de sus interacciones y relaciones con otras partes interesadas dentro de un ecosistema más amplio. Concretamente, las entidades han de adoptar las medidas oportunas para garantizar que su cooperación con las instituciones académicas y de investigación se desarrolle de acuerdo con sus políticas de ciberseguridad y siga buenas prácticas por lo que respecta a la seguridad del acceso y la divulgación de información en general y la protección de la propiedad intelectual en particular. De igual manera, dada la importancia y el valor de los datos para las actividades de las entidades, estas deben adoptar todas las medidas de ciberseguridad apropiadas cuando recurran a servicios de transformación de datos y análisis de datos de terceros.

(46) Para abordar en mayor profundidad los principales riesgos de la cadena de suministro y ayudar a las entidades que operan en los sectores incluidos en el ámbito de aplicación de la presente Directiva a gestionar adecuadamente los riesgos de ciberseguridad asociados a la cadena de suministro y los proveedores, el Grupo de Cooperación, con la participación de las autoridades nacionales pertinentes y en colaboración con la Comisión y la ENISA, debe llevar a cabo evaluaciones coordinadas sectoriales de los riesgos de la cadena de suministro, como ya se hizo en el caso de las redes 5G a raíz de la Recomendación (UE) 2019/534 sobre la ciberseguridad de las redes 5G[21], con el objetivo de identificar cuáles son los servicios, sistemas o productos de TIC críticos, las correspondientes amenazas y las vulnerabilidades de cada sector.

[21] Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G (DO L 88 de 29.3.2019, p. 42.).

(47) Las evaluaciones de los riesgos de la cadena de suministro, en función de las características del sector afectado, deben tener en cuenta tanto los factores técnicos como, en su caso, los de otra índole, en particular los definidos en la Recomendación (UE) 2019/534, en la evaluación de riesgos coordinada a escala de la UE de la seguridad de las redes 5G y en el conjunto de instrumentos de la UE para la seguridad de las redes 5G acordado por el Grupo de Cooperación. A fin de identificar las cadenas de suministro que deben ser objeto de una evaluación de riesgo coordinada, han de tenerse en cuenta los siguientes criterios: i) la medida en que las entidades esenciales e importantes utilizan servicios, sistemas o productos de TIC críticos y dependen de ellos, ii) la importancia de servicios, sistemas o productos de TIC críticos específicos para desempeñar funciones críticas o sensibles, en particular el tratamiento de datos personales, iii) la disponibilidad de servicios, sistemas o productos de TIC alternativos, iv) la resiliencia de la cadena de suministro global de servicios, sistemas o productos de TIC frente a las perturbaciones, y v) en el caso de los servicios, sistemas o productos de TIC emergentes, el peso que pueden tener en el futuro para las actividades de las entidades.

(48) Con vistas a racionalizar las obligaciones legales impuestas a los proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público y los prestadores de servicios de confianza relacionados con la seguridad de sus redes y sistemas de información, así como para que dichas entidades y sus respectivas autoridades competentes puedan beneficiarse del marco jurídico establecido por la presente Directiva (incluida la designación de un CSIRT responsable de la gestión de riesgos e incidentes, y la participación de las autoridades y los organismos competentes en el trabajo del Grupo de Cooperación y la red de CSIRT), procede incluirlas en el ámbito de aplicación de la presente Directiva. Por consiguiente, es preciso derogar las correspondientes disposiciones establecidas en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo[22] y en la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo[23] relativas a la imposición de requisitos de seguridad y notificación a estos tipos de entidades.

---

[22] 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).

[23] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

(48 *bis*) **La obligaciones en materia de seguridad que se establecen en la presente Directiva deben considerarse complementarias de los requisitos que se imponen a los prestadores de servicios de confianza en virtud del Reglamento (UE) n.º 910/2014 («Reglamento eIDAS»). Debe pedirse a los prestadores de servicios de confianza que tomen todas las medidas que resulten oportunas y necesarias para gestionar los riesgos que se plantean para sus servicios, también en relación con los proveedores y terceros confiantes, así como para notificar los incidentes de seguridad en virtud de la presente Directiva. Esas obligaciones en materia de seguridad y notificación también deberían versar sobre la protección física del servicio prestado. Sigue aplicándose el artículo 24 del Reglamento (UE) n.º 910/2014**.

(48 *bis bis*) **Los Estados miembros podrán asignar a los organismos de supervisión del Reglamento eIDAS la función de autoridad competente para los servicios de confianza, a fin de garantizar la continuación de las prácticas actuales y aprovechar los conocimientos y la experiencia adquiridos en la aplicación del Reglamento eIDAS. En los casos en que esa función se asigne a un organismo distinto, las autoridades nacionales competentes en virtud de la presente Directiva deben cooperar estrechamente, de manera oportuna, intercambiando información pertinente para garantizar la supervisión efectiva y el cumplimiento por parte de los proveedores de servicios de confianza de los requisitos establecidos en la presente Directiva y en el Reglamento [XXXX/XXXX].**

Cuando proceda, la autoridad nacional competente en virtud de la presente Directiva informará sin demora indebida al organismo de supervisión del Reglamento eIDAS de cualquier ciberamenaza o ciberincidente notificado que repercuta en los servicios de confianza, así como de cualquier incumplimiento por parte de los proveedores de los servicios de confianza de los requisitos establecidos en la presente Directiva. A efectos de notificación, los Estados miembros podrán utilizar un punto de entrada único establecido para efectuar una notificación de incidentes común y automática al organismo de supervisión del Reglamento eIDAS y a la autoridad competente en virtud de la presente Directiva. Las normas sobre las obligaciones de notificación deben entenderse sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo[24].

[24] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

(49) Cuando proceda, y para evitar perturbaciones innecesarias, las directrices nacionales existentes […] adoptadas para la transposición de las normas relacionadas con las medidas de seguridad establecidas en los artículos 40[…] y 41 de la Directiva (UE) 2018/1972[…] **deben tenerse en cuenta en las modalidades de transposición que hayan aplicado los Estados miembros en relación con la presente Directiva, apoyándose así en los conocimientos y competencias ya adquiridos en virtud de la Directiva (UE) 2018/1972, en relación con las medidas para la gestión de los riesgos de ciberseguridad y las notificaciones de incidentes. La ENISA puede elaborar directrices sobre requisitos de seguridad y notificación para los proveedores de redes públicas de comunicaciones electrónicas o los proveedores de servicios de comunicación electrónica disponibles al público, con el fin de facilitar la armonización y la transición y de minimizar las perturbaciones. Los Estados miembros pueden asignar a las autoridades nacionales de reglamentación la función de autoridad competente para las comunicaciones electrónicas, a fin de garantizar la continuación de las prácticas actuales y aprovechar los conocimientos y la experiencia adquiridos con la Directiva (UE) 2018/1972.**

(50) Dada la importancia que están adquiriendo los servicios de comunicaciones interpersonales independientes de la numeración, es necesario garantizar que estos servicios también estén sujetos a requisitos de seguridad apropiados a la vista de su naturaleza específica e importancia económica. Así, los proveedores de este tipo de servicios deben garantizar un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado. Puesto que los proveedores de servicios de comunicaciones interpersonales independientes de la numeración no suelen ejercer un control real sobre la transmisión de las señales a través de las redes, en ciertos sentidos puede considerarse que el grado de riesgo de estos servicios es inferior al de los servicios de comunicaciones electrónicas tradicionales. Lo mismo puede decirse de los servicios de comunicaciones interpersonales que utilizan números y que no ejercen un control real sobre la transmisión de la señal.

(51) Hasta ahora, el mercado interior nunca había dependido tanto del funcionamiento de internet. Los servicios de prácticamente todas las entidades esenciales e importantes dependen de servicios prestados por internet. Para garantizar que la prestación de los servicios suministrados por entidades esenciales e importantes se desarrolle sin problemas, es importante que las redes públicas de comunicaciones electrónicas, tales como las redes troncales de internet o los cables de comunicaciones submarinos, cuenten con medidas de ciberseguridad apropiadas y notifiquen los incidentes en este ámbito.

(52) Cuando […] **proceda**, las entidades deben informar a los destinatarios de su servicio de medidas […] concretas que pueden aplicar para reducir el consiguiente riesgo **de una ciberamenaza significativa** para ellos mismos. **Las autoridades, cuando corresponda, y en particular en los casos en que las ciberamenazas significativas puedan materializarse, también deben notificar la propia amenaza a los destinatarios de su servicio al mismo tiempo que a las autoridades competentes o los CSIRT.** La exigencia de informar a los destinatarios de tales amenazas no exime a las entidades de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para prevenir o subsanar cualquier ciberamenaza y restablecer el nivel normal de seguridad del servicio. El suministro de la mencionada información sobre las **ciber**amenazas […] a los destinatarios debe ser gratuito.

(53) Concretamente, los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público deben informar a los destinatarios del servicio de ciberamenazas concretas y significativas y de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones, por ejemplo, utilizar determinados tipos de soporte lógico o tecnologías de cifrado.

(54) Para salvaguardar la seguridad de las redes y servicios de comunicaciones electrónicas, debe promoverse el uso del cifrado, y en particular el cifrado de extremo a extremo, y, cuando sea necesario, debe ser obligatorio para los proveedores de tales servicios y redes de conformidad con los principios de seguridad y protección de la privacidad por defecto y desde el diseño a efectos del artículo 18. El uso de cifrado de extremo a extremo debe entenderse sin perjuicio de las facultades del Estado miembro para garantizar la protección de sus intereses de seguridad esenciales y la seguridad pública, y para permitir la investigación, detección y enjuiciamiento de infracciones penales con arreglo al Derecho de la Unión. Las soluciones que permitan acceder de manera lícita a la información contenida en comunicaciones cifradas de extremo a extremo deben mantener la eficacia del cifrado en la protección de la privacidad y la seguridad de las comunicaciones, al tiempo que proporcionan una respuesta efectiva a la delincuencia.

(55) La presente Directiva establece un enfoque en dos etapas respecto a la notificación de incidentes a fin de alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a mitigar la posible propagación de incidentes y permita a las entidades buscar apoyo, y, por el otro, una notificación en profundidad que extraiga lecciones valiosas de incidentes individuales y mejore con el tiempo la resiliencia frente a las ciberamenazas de empresas concretas y sectores completos. Cuando las entidades tengan conocimiento de un incidente, deben estar obligadas a presentar una notificación inicial en el plazo de veinticuatro horas, seguida de un informe final a más tardar un mes después. La notificación inicial solo debe incluir la información que sea estrictamente necesaria para que las autoridades competentes tengan constancia del incidente y la entidad pueda solicitar asistencia, en caso de que sea necesario. Cuando proceda, dicha notificación debe indicar si el incidente se debe a una acción presuntamente ilícita o maliciosa. Los Estados miembros deben velar por que el requisito de presentar esta notificación inicial no desvíe los recursos de la entidad notificante de actividades relacionadas con la gestión de incidentes que deban priorizarse. Por otra parte, para evitar que las obligaciones de notificación de incidentes desvíen recursos de la gestión de la respuesta al incidente o puedan comprometer de cualquier otra forma los esfuerzos de las entidades en este sentido, los Estados miembros deben prever también que, en casos debidamente justificados y de acuerdo con las autoridades competentes o el CSIRT, la entidad afectada pueda incumplir los plazos de veinticuatro horas para la notificación inicial y de un mes para el informe final.

(55 *bis*) **Adoptar un planteamiento proactivo ante las ciberamenzas es vital en la gestión de riesgos de ciberseguridad y debería posibilitar que las autoridades competentes puedan prevenir de manera efectiva que las ciberamenazas se materialicen en incidentes reales que puedan causar pérdidas materiales o morales considerables. A tal fin, es de vital importancia la notificación de ciberamenazas significativas.**

(56) Las entidades esenciales e importantes suelen verse en la situación de que un incidente concreto, por sus características, debe notificarse a diversas autoridades en cumplimiento de las obligaciones de notificación recogidas en varios instrumentos jurídicos. Estos casos crean cargas adicionales y también pueden generar inseguridad en cuanto al formato y el procedimiento de tales notificaciones. Por todo ello, y a efectos de simplificar la notificación de los incidentes de seguridad, los Estados miembros […] **podrían** establecer *un punto de entrada único* para todas las notificaciones obligatorias en virtud de la presente Directiva y también de otros actos legislativos de la Unión, como el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. La ENISA, en colaboración con el Grupo de Cooperación, debe elaborar modelos de notificación comunes mediante directrices que simplifiquen y racionalicen la información que debe notificarse con arreglo al Derecho de la Unión y reduzcan las cargas para las empresas.

(57) 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 las entidades esenciales e importantes, sobre la base de las normas aplicables de los procesos penales con arreglo al Derecho de la Unión, a denunciar ante las autoridades policiales competentes los incidentes de naturaleza presuntamente delictiva y grave. Cuando proceda, y sin perjuicio de las normas de protección de datos personales aplicables a Europol, conviene que la EC3 y la ENISA faciliten la coordinación entre las autoridades competentes y las autoridades policiales de distintos Estados miembros.

(58) En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes deben cooperar e intercambiar información sobre todas las cuestiones pertinentes con las autoridades de protección de datos y las autoridades de control en virtud de la Directiva 2002/58/CE.

(59) Mantener bases de datos precisas y completas con los nombres de dominio y los datos de registro (los denominado «datos WHOIS») y proporcionar un acceso lícito a tales datos es fundamental para garantizar la seguridad, estabilidad y resiliencia del DNS, lo que a su vez contribuye a garantizar un elevado nivel común de ciberseguridad en el seno de la Unión. Cuando el tratamiento comprenda datos personales, dicho tratamiento debe ajustarse a la legislación de la Unión en materia de protección de datos.

(60) La disponibilidad y accesibilidad oportuna de estos datos para las autoridades públicas, incluidas las autoridades competentes en virtud del Derecho nacional o de la Unión para la prevención, la investigación o el enjuiciamiento de infracciones penales, los CERT, los CSIRT y, por lo que respecta a los datos de sus clientes, los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de ciberseguridad que actúen en nombre de dichos clientes, son fundamentales para evitar y combatir los abusos del sistema de nombres de dominio, en particular para prevenir, detectar y responder a incidentes de ciberseguridad. Dicho acceso debe ser conforme con la legislación de la Unión en materia de protección de datos en la medida en que haya datos personales implicados.

(61) Al objeto de garantizar la disponibilidad de datos precisos y completos sobre el registro de nombres de dominio, los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel (los denominados «registradores») deben recabar y garantizar la integridad y disponibilidad de los datos de registro de nombres de dominio. **Por lo que se refiere a los datos de registro, las entidades deben, en particular, verificar el nombre y la dirección de correo electrónico de los titulares.** […] Los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel deben establecer políticas y procedimientos para recoger y mantener datos de registro precisos y completos, así como para prevenir y corregir datos de registro imprecisos con arreglo a las normas de protección de datos de la Unión.

(62) Los registros de dominios de primer nivel y las entidades que prestan servicios de registro de nombres de dominio para ellos deben poner a disposición del público los datos de registro de nombres de dominio que queden fuera del ámbito de aplicación de las normas de protección de datos de la Unión, como por ejemplo los datos referentes a personas jurídicas[25]. Los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel también deben permitir el acceso lícito a datos específicos sobre el registro de nombres de dominio referentes a personas físicas a solicitantes de acceso legítimos, de conformidad con el Derecho de la Unión en materia de protección de datos. Los Estados miembros deben velar por que los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel para ellos respondan sin demora indebida a las solicitudes de divulgación de datos de registro de nombres de dominio **provenientes de solicitantes de acceso legítimos, como las autoridades competentes en virtud del Derecho nacional o de la Unión en el ámbito de la seguridad nacional y de la justicia penal, o los CSIRT.** Los registros de dominios de primer nivel y las entidades que presten servicios de registro de nombres de dominio de primer nivel para ellos han de establecer políticas y procedimientos para la publicación y divulgación de datos de registro, en particular acuerdos de nivel de servicio para tramitar las solicitudes de acceso de solicitantes de acceso legítimos. El procedimiento de acceso también puede incluir el uso de una interfaz, un portal u otra herramienta técnica que proporcione un sistema eficiente para la solicitud de datos de registro y el acceso a ellos. **Los Estados miembros deben garantizar que todos los tipos de acceso a los datos de registro de dominios (tanto datos personales como no personales) sean gratuitos.** Con vistas a promover prácticas armonizadas en todo el mercado interior, la Comisión podrá adoptar directrices sobre dichos procedimientos sin perjuicio de las competencias del Comité Europeo de Protección de Datos, **de conformidad y en complementariedad con las normas internacionales elaboradas por la comunidad multilateral**.

---

25 El considerando 14 del Reglamento (UE) 2016/679 **d**[...]el Parlamento Europeo **y**[...] **d**el[...] Consejo dispone que «[e]l presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto».

(63) […]**L**as entidades esenciales e importantes en virtud de la presente Directiva deben estar sometidas a la jurisdicción del Estado miembro en el que prestan sus servicios. **Las entidades indicadas en los puntos 1 a 7 y 10 del Anexo I, los prestadores de servicios de confianza y los proveedores de puntos de intercambio de internet indicados en el punto 8 del anexo I y en los puntos 1 a 5 del anexo II de la presente Directiva deben estar sometidos a la jurisdicción del Estado miembro en el que estén establecidos.** Si la entidad presta servicios **o tiene un establecimiento** en más de un Estado miembro, debe estar sometida a la jurisdicción separada y concurrente de cada uno de ellos. Las autoridades competentes de estos Estados miembros deben cooperar, prestarse asistencia mutua y, cuando proceda, emprender medidas conjuntas de supervisión. **Cuando los Estados miembros decidan ejercer su competencia, deben evitar que una misma conducta sea sancionada más de una vez por la infracción de las obligaciones establecidas en la presente Directiva.**

(64) A fin de tener en cuenta la naturaleza transfronteriza de los servicios y operaciones de los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel **y las entidades que proporcionen registros de nombres de dominio para estos**, los proveedores de redes de distribución de contenidos, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de servicios digitales, solo un Estado miembro debe tener jurisdicción sobre estas entidades. La jurisdicción debe atribuirse al Estado miembro en el que se encuentre el establecimiento principal en la Unión de la respectiva entidad. El criterio de establecimiento a los efectos de la presente Directiva implica el ejercicio 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.

El cumplimiento de este criterio no debe depender de que las redes y sistemas de información se encuentren físicamente en un lugar determinado; la presencia y utilización de tales sistemas no constituyen, por sí mismas, dicho establecimiento principal y, por tanto, no son criterios decisivos para determinar el establecimiento principal. El establecimiento principal debe ser el lugar en el que se toman **predominantemente** las decisiones relativas a las medidas para la gestión de riesgos de ciberseguridad dentro de la Unión, que habitualmente coincidirá con el lugar en que se encuentra la administración central de las empresas en la Unión. En caso de que **no se pueda determinar el lugar en el que se toman predominantemente dichas decisiones o que estas** no se adopten dentro de la Unión, debe considerarse que el establecimiento principal se encuentra en el Estado miembro en el que la entidad tiene el establecimiento con mayor número de trabajadores en la Unión. Cuando los servicios los preste un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial.

(64 *bis*) Cuando un proveedor de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público presta un servicio de DNS recursivo solamente como parte del servicio de acceso a internet, la entidad se debe considerar bajo la competencia de todos los Estados miembros en los que presta sus servicios.

(64 *bis bis*) Con objeto de proporcionar una visión global clara de los proveedores de servicios DNS, los registros de nombres de dominio de primer nivel, los proveedores de redes de distribución de contenidos, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de servicios digitales en toda la Unión en el ámbito de aplicación de la presente Directiva, la ENISA debe crear y mantener un registro para dichas entidades, a partir de las notificaciones recibidas por los Estados miembros, según proceda por medio de sus mecanismos nacionales de autonotificación. Con objeto de asegurar la exactitud y exhaustividad de la información que se debe incluir en el registro, los Estados miembros deben presentar a la ENISA la información disponible en sus registros sobre estas entidades. La ENISA y los Estados miembros deben tomar medidas que faciliten la interoperabilidad de estos registros y además aseguren la protección de la información confidencial o clasificada.

(65) En situaciones en las que los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de redes de distribución de contenidos, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos y los proveedores de servicios digitales no estén establecidos en la Unión pero ofrezcan servicios dentro de ella, deben designar un representante. Para determinar si dicha entidad ofrece servicios en la Unión, debe averiguarse si hay constancia de que la entidad tiene la intención de ofrecer servicios a personas de uno o varios Estados miembros. La simple accesibilidad en la Unión del sitio web de la entidad 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 establecida la entidad, 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 la entidad tiene la intención de ofrecer servicios en la Unión. El representante debe actuar por cuenta de la entidad, 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 de la entidad que le autorice para actuar por cuenta de esta en lo que respecta a las obligaciones de la entidad en virtud de la presente Directiva, también por lo que respecta a la notificación de incidentes.

(66) Cuando se intercambie, notifique o comparta de cualquiera forma en virtud de las disposiciones de la presente Directiva información que se considere clasificada de acuerdo con el Derecho nacional o de la Unión, deben aplicarse las correspondientes normas específicas sobre el tratamiento de información clasificada.

(67) Puesto que las ciberamenazas son cada vez más complejas y sofisticadas, el éxito de las medidas de detección y prevención depende en gran medida de que las entidades compartan regularmente información sobre las amenazas y las vulnerabilidades. El intercambio de información contribuye a crear una mayor conciencia sobre las ciberamenazas, lo que a su vez refuerza la capacidad de las entidades para evitar que las amenazas se materialicen en incidentes reales y les permite contener mejor los efectos de los incidentes y recuperarse de manera más eficiente. Ante la ausencia de orientación a nivel de la Unión, son varios los factores que parecen haber dificultado este intercambio de información, en particular la incertidumbre en cuanto a la compatibilidad con las normas sobre competencia y responsabilidad.

(68) Debe animarse a las entidades a aprovechar colectivamente sus conocimientos y experiencias prácticas individuales a nivel estratégico, táctico y operativo para reforzar sus capacidades a fin de evaluar y realizar un seguimiento de las ciberamenazas, defenderse de ellas y reaccionar en consecuencia. Por consiguiente, es necesario propiciar la creación a nivel de la Unión de mecanismos para los acuerdos voluntarios de intercambio de información. Para ello, los Estados miembros también deben apoyar y alentar activamente a las entidades pertinentes que no estén incluidas en el ámbito de aplicación de la presente Directiva para que participen en tales mecanismos de intercambio de información. El funcionamiento de dichos mecanismos debe ajustarse plenamente a las normas en materia de competencia de la Unión, así como a las normas del Derecho de la Unión relativas a la protección de datos.

(69) […] **E**n la medida en que sea estrictamente necesario y proporcionado a efectos de garantizar la seguridad de las redes y de la información**, el tratamiento de datos personales** por parte de entidades […] y proveedores de tecnologías y servicios de seguridad **esenciales e importantes se puede considerar necesario para cumplir con una obligación jurídica o** […] puede constituir un interés legítimo del responsable del tratamiento de que se trate **[…]**, tal como se contempla en el Reglamento (UE) 2016/679 Ello **puede** […] incluir medidas relacionadas con la prevención, la detección y el análisis de incidentes y la respuesta ante estos, medidas para incrementar el conocimiento relacionado con ciberamenazas específicas, el intercambio de información en el contexto de la corrección y divulgación coordinada de las vulnerabilidades, incluido el intercambio voluntario de información sobre dichos incidentes, así como ciberamenazas y vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración. Dichas medidas pueden requerir el tratamiento de […] **diversos** tipos de datos personales**, como por ejemplo**: direcciones IP, localizadores unificados de recursos (URL), nombres de dominio y direcciones de correo electrónico. **El tratamiento de datos personales por parte de las autoridades competentes, los puntos nacionales de contacto único para la ciberseguridad y los equipos de respuesta a incidentes de seguridad informática (CSIRT) se deben establecer en la legislación nacional y se deben considerar necesarios para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, según se indica en el artículo 6, apartado 1, letras c) o e) del Reglamento (UE) 2016/679.**

(69 *bis*) Las legislaciones de los Estados miembros pueden establecer normas que permitan a las autoridades competentes, a los puntos nacionales de contacto único para la ciberseguridad y a los CSIRT tratar categorías especiales de datos personales de conformidad con el artículo 9[…] del Reglamento (UE) 2016/679, en la medida en que sea estrictamente necesario y proporcionado para garantizar la seguridad de las redes y los sistemas de información de las entidades esenciales e importantes, concretamente proporcionando medidas adecuadas y concretas para salvaguardar los derechos fundamentales y los intereses de las personas físicas, en particular las limitaciones técnicas sobre la reutilización de dichos datos y la utilización de medidas de seguridad y de protección de la privacidad de última generación, como por ejemplo la seudonimización, o la encriptación en casos en que la anonimización pueda repercutir considerablemente sobre el objetivo deseado.

(70) Con vistas a reforzar las facultades y las medidas de supervisión que ayudan a garantizar un cumplimiento efectivo, la presente Directiva debe prever una lista mínima de actuaciones y medios de supervisión a través de los cuales las autoridades competentes puedan supervisar a las entidades esenciales e importantes. Además, la presente Directiva debe establecer una diferenciación respecto al régimen de supervisión entre las entidades esenciales y las entidades importantes con vistas a garantizar un equilibrio justo de las obligaciones para las entidades y las autoridades competentes. En consecuencia, las entidades esenciales deben estar sujetas a un régimen de supervisión completo (*a priori* y *a posteriori*), mientras que las entidades importantes deben estar sujetas a un régimen de supervisión menos estricto exclusivamente *a posteriori*. En este último caso, implica que las entidades importantes no **tengan la obligación de** […] documentar sistemáticamente la conformidad con los requisitos de gestión de riesgos de ciberseguridad y que las autoridades competentes deben aplicar un enfoque reactivo *a posteriori* respecto a la supervisión y, por ende, no tienen la obligación general de supervisar a dichas entidades. **En el caso de entidades importantes, la supervisión *a posteriori* puede iniciarse cuando las autoridades competentes hayan recibido pruebas o indicios o información que dichas autoridades estimen que puede considerarse un posible incumplimiento de las obligaciones establecidas en la presente Directiva. Por ejemplo, estas pruebas, indicios o información podrían ser del tipo transmitido a las autoridades competentes por otras autoridades, entidades, ciudadanos, medios de comunicación u otras fuentes, o información disponible para el público, o puede recibirse por otras actividades realizadas por las autoridades competentes en el ejercicio de sus funciones.**

(70 *bis*) En el ejercicio de la supervisión *a priori*, las autoridades competentes deben poder decidir sobre la priorización de la utilización de las medidas de supervisión y de los medios a su disposición de manera proporcionada. Esto supone que las autoridades competentes pueden decidir sobre dicha priorización a partir de las metodologías de supervisión que deben aplicar un planteamiento basado en el riesgo. Concretamente, estas metodologías pueden incluir criterios o indicadores para la clasificación de entidades esenciales en categorías de riesgo con las correspondientes medidas de supervisión y medios recomendados para cada categoría de riesgo, tales como el uso, la frecuencia o el tipo de inspecciones *in situ* o auditorías de seguridad específicas o análisis de seguridad, el tipo de información que se debe solicitar y el nivel de detalle de dicha información. Estas metodologías de supervisión también se pueden complementar con programas de trabajo y se pueden evaluar y revisar de manera periódica, en particular en aspectos tales como la dotación de recursos y las necesidades.

(70 *bis bis*) En lo relativo a las entidades de la Administración pública, las facultades de supervisión se pueden aplicar en consonancia con los marcos nacionales y con el ordenamiento jurídico. Los Estados miembros deben tener capacidad para decidir sobre la imposición de medidas de supervisión y ejecución que sean adecuadas, proporcionadas y eficaces en relación con estas entidades.

(70 *bis bis bis*) Los Estados miembros pueden exigir a entidades esenciales e importantes la utilización de servicios de confianza cualificados o sistemas de identificación electrónica notificados con arreglo al Reglamento (UE) n.º 910/2014, con objeto de demostrar el cumplimiento de determinadas medidas de gestión de riesgos de ciberseguridad.

(71) A fin de garantizar el cumplimiento efectivo, debe fijarse una lista mínima de sanciones administrativas por la infracción de las obligaciones de gestión de riesgos de ciberseguridad y notificación previstas en la presente Directiva, mediante el establecimiento de un marco claro y coherente para tales sanciones en toda la Unión. Debe prestarse la debida atención a la naturaleza, gravedad y duración de la infracción, los perjuicios o las pérdidas reales originados, o los perjuicios o las pérdidas que podrían haberse originado, la intencionalidad o negligencia en la infracción, las medidas adoptadas para prevenir o paliar los perjuicios o las pérdidas sufridos, el grado de responsabilidad o cualquier infracción anterior pertinente. el grado de cooperación con la autoridad competente y cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(71 *bis*) Las disposiciones relativas a la responsabilidad de las personas físicas que detentan determinadas responsabilidades dentro de una entidad por faltar a su deber de asegurar el cumplimiento de las obligaciones establecidas en la presente Directiva no exigen que los Estados miembros abran una causa penal o de responsabilidad civil por los daños ocasionados a terceras partes por dicha falta.

(72) A fin de garantizar el cumplimiento efectivo de las obligaciones contempladas en la presente Directiva, cada autoridad competente debe estar facultada para imponer multas administrativas o solicitar su imposición.

(73) Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, a la hora de valorar la cuantía apropiada de la multa el nivel la autoridad de supervisión debe tener en cuenta el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. Debe corresponder a los Estados miembros determinar si se debe imponer multas administrativas a las autoridades públicas y en qué medida. La imposición de una multa administrativa no afecta al ejercicio de otras facultades de las autoridades competentes ni a la aplicación de otras sanciones contempladas en las normas nacionales que transpongan la presente Directiva.

(74) Los Estados miembros […] **pueden** establecer las normas sobre las sanciones penales por infracciones de las normas nacionales que transpongan la presente Directiva. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas asociadas no debe entrañar la vulneración del principio *ne bis in idem*, según la interpretación del Tribunal de Justicia.

(75) En los casos en que la presente Directiva no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves de las obligaciones establecidas en la presente Directiva, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(76) Con vistas a reforzar más aun la eficacia y el carácter disuasorio de las sanciones aplicables por la infracción de las obligaciones establecidas en virtud de la presente Directiva, las autoridades competentes deben estar facultadas para aplicar sanciones que consistan en la suspensión de una certificación o autorización referente a una parte o la totalidad de los servicios prestados por una entidad esencial y la imposición de una prohibición temporal de que una persona física ejerza funciones de dirección. Habida cuenta de su gravedad y repercusión en las actividades de las entidades y, en última instancia, en sus consumidores, dichas sanciones deben aplicarse exclusivamente de manera proporcional a la gravedad de la infracción y teniendo en cuenta las circunstancias específicas de cada caso, incluida la intencionalidad o negligencia en la infracción y las medidas adoptadas para prevenir o paliar los daños o perjuicios sufridos. Las sanciones solo deben aplicarse como ultima ratio, es decir, únicamente después de haber agotado el resto de medidas de ejecución pertinentes establecidas por la presente Directiva y exclusivamente por el tiempo hasta que las entidades a las que se aplican adopten las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente en nombre de la que se aplicaron dichas sanciones. La imposición de tales sanciones estará sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta de los Derechos Fundamentales de la Unión Europea, entre ellas el derecho a la tutela judicial efectiva, a la presunción de inocencia y a un proceso con todas las garantías.

(76 *bis*) Con el fin de asegurar la eficacia de la supervisión y la ejecución, especialmente en casos con dimensión transfronteriza, los Estados miembros que hayan recibido una solicitud de asistencia mutua deben, en la medida en que lo exprese la solicitud, tomar medidas de supervisión y ejecución adecuadas en relación con la entidad en cuestión que presta servicios o que tiene la red y el sistema de información en su territorio.

(77) La presente Directiva debe establecer normas de cooperación entre las autoridades competentes y las autoridades de control con arreglo al Reglamento (UE) 2016/679 para tratar las infracciones relacionadas con los datos personales.

(78) La presente Directiva debe aspirar a garantizar un nivel elevado de responsabilidad por las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación a nivel de las organizaciones. Por estos motivos, los órganos de dirección de las entidades incluidas en el ámbito de aplicación de la presente Directiva deben aprobar las medidas de gestión de los riesgos de ciberseguridad y supervisar su aplicación.

(79) Debe introducirse un […]**sistema** de […] **aprendizaje** entre iguales que **ayude a reforzar la** confianza **mutua** y **a aprender de las buenas prácticas y la experiencia**, y que permita […] **intercambios entre iguales por** expertos designados por los Estados miembros **sobre** […] la aplicación de las políticas de ciberseguridad […]. **Al aplicar el sistema de aprendizaje entre iguales se debe prestar especial atención a asegurar que no supone una carga innecesaria o desproporcionada para las autoridades pertinentes de los Estados miembros. La Comisión debe estudiar todas las posibilidades de garantizar la cobertura financiera de los gastos resultantes de la organización de misiones de aprendizaje entre iguales. Asimismo, el sistema de aprendizaje entre iguales debe tener en cuenta los resultados de instrumentos parecidos, como el sistema de revisión entre iguales de la red de CSIRT, añadir valor y evitar duplicaciones. La ejecución del sistema de aprendizaje entre iguales se debe entender sin perjuicio de la legislación nacional o de la Unión relativa a la protección de información confidencial y clasificada. Antes del inicio de las sesiones de aprendizaje entre iguales, los Estados miembros pueden realizar una autoevaluación de los aspectos pertinentes. La ENISA puede proporcionar orientaciones sobre la autoevaluación y las plantillas pertinentes, en su caso, previa solicitud del Grupo de Cooperación. Los Estados miembros pueden decidir poner sus informes respectivos a disposición del público.**

(80) […]

(81) A fin de garantizar condiciones uniformes de ejecución de las disposiciones pertinentes de la presente Directiva sobre las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Cooperación, los elementos técnicos relacionados con las medidas de gestión de riesgos o el tipo de información, el formato y el procedimiento de las notificaciones de los incidentes**, y las categorías de entidades a las que se les exigirá emplear determinados productos, servicios y procesos de TIC certificados**, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo.[26]

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

[26] 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).

(83) Dado que el objetivo de la presente Directiva, a saber, garantizar un elevado nivel común de ciberseguridad 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.

(84) 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 con arreglo a esos derechos y principios.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

1. La presente Directiva establece medidas destinadas a garantizar un elevado nivel común de ciberseguridad dentro de la Unión **con el objetivo de mejorar el funcionamiento del mercado interior**.

2. A tal fin, la presente Directiva:

   a) establece obligaciones por las cuales los Estados miembros deben adoptar estrategias nacionales de ciberseguridad y designar autoridades nacionales competentes, puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT);

   b) establece obligaciones de gestión de riesgos de ciberseguridad y notificación para las entidades a cuyos tipos se hace referencia […] en **los** anexos I **y II** […];

   c) establece **normas y** obligaciones relativas al intercambio de información sobre ciberseguridad.

Artículo 2

Ámbito de aplicación

1. La presente Directiva se aplica a las entidades públicas y privadas de **los** tipo**s enumerados** […] en **los** anexos I **y II** […] **que alcancen o superen los límites máximos establecidos para las empresas medianas** […] en el sentido de la Recomendación 2003/361/CE de la Comisión[27]. **El artículo 3, apartado 4, y el artículo 6, apartado 2, párrafos segundo y tercero, del anexo de dicha Recomendación no se aplicarán a efectos de la presente Directiva.**

2. […] **I**ndependientemente del […] tamaño **de las entidades a que se refiere el apartado 1**, la presente Directiva se aplica también **cuando:** […]

   a) los servicios sean prestados por una de las siguientes entidades:

      i) **proveedores de** redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público a que se refiere el anexo I, punto 8,

      ii) **prestadores cualificados de servicios de confianza a que se refiere el anexo I, punto XX,**

      iii) **prestadores no cualificados de servicios de confianza a que se refiere el anexo I, punto XX,**

      iv) registros de nombres de dominio de primer nivel […] a que se refiere el anexo I, punto 8;

   b) […]

[27] 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).

c) la entidad sea el único proveedor **en un Estado miembro** de un servicio […] **esencial para el mantenimiento de actividades económicas o sociales críticas**;

d) una posible perturbación del servicio prestado por la entidad pudiera tener repercusiones **significativas** sobre la seguridad pública, el orden público o la salud pública;

e) una posible perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos **significativos**, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo;

f) […];

g) la entidad se identifique como entidad crítica en virtud de la Directiva (UE) XXXX/XXXX del Parlamento Europeo y del Consejo[28] [Directiva sobre la resiliencia de las entidades críticas] **[**o como una entidad equivalente a una entidad crítica con arreglo al artículo 7 de dicha Directiva**]**.

2 *bis*. Independientemente de su tamaño, la Directiva también se aplica a las entidades públicas de la administración central reconocidas como tales en un Estado miembro de conformidad con la legislación nacional y mencionados en el anexo I, punto 9. Los Estados miembros podrán establecer que la presente Directiva se aplique también a las entidades públicas de las administraciones regionales y locales.

28 [insértese el título completo y la referencia de publicación en el DO cuando se conozcan].

3. […]

La presente Directiva se entiende sin perjuicio de las responsabilidades de los Estados miembros de salvaguardar la seguridad nacional o de sus competencias de salvaguardar otras funciones esenciales del Estado, como garantizar la integridad territorial del Estado o mantener la ley y el orden.

3 *bis*. 1. La presente Directiva no se aplica a:

a) entidades que no entren dentro del ámbito de aplicación del Derecho de la Unión y, en todo caso, a todas las entidades que lleven a cabo principalmente actividades en los ámbitos de la defensa, la seguridad nacional, la seguridad pública o actividades policiales, independientemente de qué entidad esté llevando a cabo estas actividades y de si se trata de una entidad pública o privada, sin perjuicio del apartado 2.

b) entidades que lleven a cabo actividades en los ámbitos del poder judicial, los parlamentos o los bancos centrales. […]

2. Cuando las entidades de la administración pública lleven a cabo actividades en estos ámbitos solo como una parte de sus actividades generales, quedarán excluidas en su totalidad del ámbito de aplicación de la presente Directiva.

3 *bis bis*. La presente Directiva no se aplica a:

i) actividades o entidades que estén excluidas del ámbito de aplicación del Derecho de la Unión y, en todo caso, a todas las actividades relacionadas con la seguridad nacional o la defensa, independientemente de qué entidad lleve a cabo dichas actividades y de si se trata de una entidad pública o privada;

ii) actividades o entidades en el ámbito del poder judicial, los parlamentos, los bancos centrales y la seguridad pública, incluidas las entidades de la administración pública que lleven a cabo actividades policiales a efectos de la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales.

3 *bis bis bis*. Las obligaciones establecidas en la presente Directiva no implican el suministro de información cuya divulgación sea contraria a los intereses esenciales de los Estados miembros en materia de seguridad nacional, seguridad pública o defensa.

3 *bis bis bis bis*.La presente Directiva se entiende sin perjuicio de la legislación de la Unión relativa a la protección de los datos de carácter personal, en particular el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE.

3 *ter*. La presente Directiva no se aplica a entidades que estén exentas de las disposiciones del Reglamento (UE) XXXX/XXXX del Parlamento Europeo y del Consejo [Reglamento sobre la resiliencia operativa digital del sector financiero], de conformidad con el artículo 2, apartado 4, del Reglamento sobre la resiliencia operativa digital del sector financiero.

4. La presente Directiva se entenderá sin perjuicio de […][29] […] las Directivas 2011/93/UE[30] y 2013/40/UE[31] 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 **de conformidad con la presente Directiva** 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. El intercambio de información preservará la confidencialidad de esta y protegerá la seguridad y los intereses comerciales de las entidades esenciales o importantes.

---

29 […]

30 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).

31 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).

Artículo 2 **bis**

Entidades esenciales e importantes

1. De las entidades a las que se aplica la presente Directiva, se considerarán esenciales las siguientes:

i) entidades de un tipo contemplado en los puntos 1 a 8 *bis* y 10 del anexo I de la presente Directiva que superen los límites máximos establecidos para las empresas medianas en la Recomendación 2003/361/CE de la Comisión;

ii) las entidades medianas a que se refiere el artículo 2, apartado 2, letra a), inciso i);

iii) las entidades a que se refiere el artículo 2, apartado 2, letra a), incisos ii) y iv) de la presente Directiva, independientemente de su tamaño;

iv) las entidades a que se refiere el artículo 2, apartado 2, letra g), y el artículo 2, apartado 2 *bis*, de la presente Directiva, independientemente de su tamaño;

v) si así lo disponen los Estados miembros, las entidades identificadas por los Estados miembros antes de la entrada en vigor de la presente Directiva como operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 o la legislación nacional;

vi) las entidades que excedan los límites máximos establecidos para las empresas medianas definidos en la Recomendación 2003/361/CE de la Comisión del tipo al que se refiere el anexo II que los Estados miembros determinen como esenciales sobre la base de los criterios previstos en el artículo 2, apartado 2, letras c), d) y e);

vii) entidades medianas en el sentido de la Recomendación 2003/361/CE de la Comisión que los Estados miembros determinen como esenciales sobre la base de los criterios previstos en el artículo 2, apartado 2, letras c), d) y e);

viii) entidades pequeñas o microentidades en el sentido de la Recomendación 2003/361/CE de la Comisión a que se refiere el apartado 2, letra a), inciso i), o definidas en virtud del apartado 2, letras c), d) y e) de dicho artículo que los Estados miembros determinen como esenciales sobre la base de evaluaciones de riesgos nacionales.

2. De las entidades a las que se aplica la presente Directiva, se considerarán importantes las siguientes:

i) entidades de un tipo contemplado en el anexo I de la presente Directiva que tengan la consideración de empresas medianas en el sentido de la Recomendación 2003/361/CE de la Comisión y entidades del tipo contemplado en el anexo II que alcancen o superen los límites máximos establecidos para las empresas medianas en el sentido de la Recomendación 2003/361/CE de la Comisión[32];

ii) las entidades a que se refiere el artículo 2, apartado 2, inciso iii), de la presente Directiva, independientemente de su tamaño;

iii) las entidades pequeñas y microentidades a que se refiere el artículo 2, apartado 2, letra a), inciso i);

iv) las entidades pequeñas y microentidades que los Estados miembros consideren importantes sobre la base del artículo 2, apartado 2, letras c), d) y e).

---

32 **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).**

Artículo 2 **bis**

Mecanismos de notificación

1. **Los Estados miembros podrán establecer mecanismos nacionales de autonotificación que requieran a todas las entidades incluidas en el ámbito de aplicación de la presente Directiva que faciliten al menos su nombre, dirección, datos de contacto, el sector en el que operan o el tipo de servicio que prestan y, en su caso, la lista de Estados miembros en los que prestan servicios sujetos a la presente Directiva a las autoridades competentes en virtud de la presente Directiva o a los organismos designados a tal efecto por los Estados miembros.**

2. Los Estados miembros […] facilitarán a la Comisión, **en relación con las entidades que hayan determinado con arreglo al artículo 2, apartado 2, letras b) a e), al menos información pertinente sobre el número de entidades determinadas, el sector al que pertenecen o el tipo de servicio que prestan según los anexos, y la disposición y las disposiciones del artículo 2, apartado 2, de acuerdo con las cuales fueron determinadas a más tardar [doce meses después del plazo límite de transposición de la presente Directiva].** […] Los Estados miembros revisarán periódicamente […] **esta información** […], y al menos cada dos años en lo sucesivo, y la actualizarán cuando proceda.

Artículo 2 **ter**

Actos sectoriales de la Unión

1. Cuando […] los actos **jurídicos** de carácter sectorial de la Unión […] exijan que las entidades esenciales o importantes adopten medidas para la gestión de riesgos de ciberseguridad o notifiquen los incidentes o las ciberamenazas **significativos** y dichos requisitos tengan un efecto al menos equivalente al de las obligaciones establecidas en la presente Directiva, no se aplicarán **a estas entidades** las disposiciones pertinentes de la presente Directiva, **incluidas las relativas a la supervisión y la ejecución recogidas en el capítulo VI**. **Si los actos jurídicos sectoriales de la Unión no cubren a todas las entidades de un sector concreto incluidas en el ámbito de aplicación de la presente Directiva, las disposiciones pertinentes de la presente Directiva seguirán aplicándose a las entidades no cubiertas por las disposiciones sectoriales en cuestión.**

2. Los requisitos a que se refiere el apartado 1 del presente artículo se considerarán equivalentes en cuanto a sus efectos a las obligaciones contempladas en la presente Directiva si el acto jurídico sectorial de la Unión correspondiente prevé el acceso inmediato, y automático y directo cuando corresponda, a las notificaciones de incidentes por parte de las autoridades competentes con arreglo a la presente Directiva o de los equipos de respuesta a incidentes de seguridad informática (CSIRT) designados, y si:

a) las medidas para la gestión de riesgos de ciberseguridad son al menos equivalentes en sus efectos a las previstas en el artículo 18, apartados 1 y 2, de la presente Directiva; o

b) los requisitos relativos a la notificación de incidentes significativos son al menos equivalentes en sus efectos a los previstos en el artículo 20, apartados 1 a 6.

3. La Comisión revisará periódicamente la aplicación de los requisitos de efecto equivalente previstos en los apartados 1 y 2 del presente artículo en relación con las disposiciones sectoriales de los actos jurídicos de la Unión. La Comisión consultará al Grupo de Cooperación y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) cuando elabore estas revisiones periódicas.

Artículo 3

Armonización mínima

Sin perjuicio del resto de sus obligaciones en virtud del Derecho de la Unión, los Estados miembros podrán […] adoptar o mantener disposiciones que garanticen un nivel más elevado de ciberseguridad **en los ámbitos cubiertos por la presente Directiva**.

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, punto 1, de la Directiva (UE) 2018/1972,

   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,

   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 los sistemas de información de resistir, con un nivel determinado de fiabilidad, **cualquier suceso** que **pueda comprometer** […] la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o **de** los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos;

2 *bis*) «servicios de comunicaciones electrónicas»: […] servicios de comunicaciones electrónicas en el sentido del artículo 2, punto 4, de la Directiva (UE) 2018/1972;

3) «ciberseguridad»: ciberseguridad en el sentido del artículo 2, punto 1, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[33];

4) «estrategia nacional de **ciberseguridad**»: marco coherente de un Estado miembro que establece una gobernanza para alcanzar las prioridades y objetivos estratégicos […] **en el ámbito de la ciberseguridad** […] en dicho Estado miembro;

5) «incidente»: todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios […] ofrecidos por redes y sistemas de información o accesibles a través de ellos;

5 *bis*) «incidente de ciberseguridad a gran escala»: un incidente con consecuencias significativas al menos en dos Estados miembros o cuyas perturbaciones excedan la capacidad de un Estado miembro para darles respuesta;

---

33 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15).

6) «gestión de incidentes»: conjunto de medidas y procedimientos destinados a detectar, analizar y limitar un incidente y responder ante este;

6 *bis*) «riesgo»: las posibles pérdidas o perturbaciones causadas por un incidente, que debe expresarse como una combinación de la magnitud de tales pérdidas o perturbaciones y la probabilidad de que se produzca dicho incidente;

7) «ciberamenaza»: una ciberamenaza en el sentido del artículo 2, punto 8, del Reglamento (UE) 2019/881;

7 *bis*) «ciberamenaza significativa»: una ciberamenaza que, basándose en sus características técnicas, cabe pensar que tiene el potencial de perturbar gravemente la red y los sistemas de información de una entidad o de sus usuarios causando pérdidas materiales o inmateriales considerables;

8) «vulnerabilidad»: deficiencia, susceptibilidad o fallo de un activo o un sistema […] de tecnologías de la información y las comunicaciones que puede ser aprovechado por una ciberamenaza;

8 *bis*) «cuasiincidente»: un suceso que, potencialmente, podría haber dañado la red y los sistemas de información de una entidad o de sus usuarios, pero cuya materialización completa se previno con éxito;

9) «representante»: toda persona física o jurídica establecida en la Unión que ha sido designada expresamente para actuar por cuenta de i) un proveedor de servicios de DNS, un registro de nombres de dominio de primer nivel, un proveedor de servicios de computación en nube, un proveedor de servicios de centro de datos o un proveedor de redes de distribución de contenidos contemplado en el anexo I, punto 8, o de ii) entidades contempladas en el anexo II, punto […] **6**, que no estén establecidas en la Unión, a las que puede dirigirse una autoridad competente nacional o un CSIRT en sustitución de la entidad, en lo que respecta a las obligaciones de dicha entidad en virtud de la presente Directiva;

10) «norma»: una norma en el sentido del artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo[34];

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

12) «punto de intercambio de internet (IXP)»: una instalación de la red que permite interconectar más de dos redes independientes (sistemas autónomos), 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, no modifica dicho tráfico ni interfiere de otra forma en el mismo;

13) «sistema de nombres de dominio (DNS)»: un sistema de nombres distribuido jerárquicamente que permite a los usuarios finales acceder a los servicios y recursos de internet;

14) «proveedor de servicios de DNS»: una entidad que presta servicios de resolución recursiva o autoritativa de nombres de dominio […] **para uso de terceros, a excepción de los servidores raíz** […];

---

34 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).

15) «registro de nombres de dominio de primer nivel»: una entidad en la que se ha delegado un dominio de primer nivel específico y que es responsable de administrar dicho dominio, incluido el registro de nombres de dominio en el dominio de primer nivel y el funcionamiento técnico del dominio de primer nivel, en particular la explotación de sus servidores de nombre, el mantenimiento de sus bases de datos y la distribución de los archivos de zona del dominio de primer nivel entre los servidores de nombre, **excluyendo al mismo tiempo las situaciones en las que los nombres de dominio de primer nivel son empleados por un registro exclusivamente para uso propio**;

15 *bis*) «entidades que prestan servicios de registro de nombres de dominio de primer nivel»: registros de nombres de dominio de primer nivel, registradores de los dominios de primer nivel y agentes de los registradores, como revendedores y prestadores de servicios de representación;

16) «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[35];

16 *bis*) «servicios de confianza»: servicios de confianza en el sentido del artículo 3, punto 16, del Reglamento (UE) n.º 910/2014;

[35] 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).

16 *ter*) «prestador cualificado de servicios de confianza »: un prestador cualificado de servicios de confianza en el sentido del artículo 3, punto 20, del Reglamento (UE) n.º 910/2014;

17) «mercado en línea»: un servicio digital en el sentido del artículo 2, letra n), de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo[36];

18) «motor de búsqueda en línea»: un servicio digital en el sentido del artículo 2, punto 5, del Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo[37];

19) «servicio de computación en nube»: un servicio digital que hace posible la administración bajo demanda y el acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos […] que se pueden compartir, **también cuando estos recursos se distribuyen en varias ubicaciones**;

20) «servicio de centro de datos»: un servicio que engloba las estructuras, o agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de las tecnologías de la información y los equipos de red que proporcionan servicios de almacenamiento, tratamiento y transporte de datos, junto con todas las instalaciones e infraestructuras necesarias para la distribución de la energía y el control ambiental;

---

36 Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») (DO L 149 de 11.6.2005, p. 22).

37 Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (DO L 186 de 11.7.2019, p. 57).

21) «red de distribución de contenidos»: una red de servidores distribuidos geográficamente a efectos de garantizar una elevada disponibilidad, accesibilidad o distribución rápida de contenidos y servicios digitales a los usuarios de internet en nombre de los proveedores de contenidos y servicios;

22) «plataforma de servicios de redes sociales»: una plataforma que permite que los usuarios finales se conecten, compartan, descubran y se comuniquen entre sí a través de múltiples dispositivos y, en particular, mediante chats, publicaciones, vídeos y recomendaciones;

23) «entidad de la Administración pública»: una entidad **reconocida como tal en un Estado miembro de conformidad con la legislación nacional** […] que cumple los siguientes criterios:

a) se ha creado para satisfacer necesidades de interés general y no tiene carácter industrial o mercantil,

b) está dotada de personalidad jurídica **o está autorizada por la ley a actuar en nombre de otra entidad dotada de personalidad jurídica**,

c) está mayoritariamente financiada por el Estado, la autoridad regional u otras entidades de Derecho público; o bien, cuya gestión se halla sometida a un control por parte de estas autoridades o entidades; o cuyos órganos de administración, de dirección o de supervisión están compuestos por miembros más de la mitad de los cuales sean nombrados por el Estado, la autoridad regional u otras entidades de Derecho público,

d) tiene facultad para dirigir a las personas físicas o jurídicas resoluciones administrativas o reglamentarias que afectan a sus derechos en la circulación transfronteriza de personas, bienes, servicios o capital;

24) «entidad»: toda persona física o jurídica constituida y reconocida como tal en virtud del Derecho nacional de su lugar de establecimiento y que, actuando en nombre propio, puede ejercer derechos y estar sujeta a obligaciones;

25) «entidad esencial»: una entidad de un tipo […] **previsto en el anexo I y designada como «esencial» de conformidad con el artículo 2 *bis*, apartado 1**;

26) «entidad importante»: una entidad del tipo […] **previsto en los anexos I y II y designada como «importante» de conformidad con el artículo 2 *bis*, apartado 2**;

26 *bis*) «producto de TIC»: un producto de TIC en el sentido del artículo 2, punto 12, del Reglamento (UE) n.º 2019/881;

26 *bis bis*) «servicio de TIC»: un servicio de TIC en el sentido del artículo 2, punto 13, del Reglamento (UE) 2019/881;

26 *bis ter*) «proceso de TIC»: un proceso de TIC en el sentido del artículo 2, punto 14, del Reglamento (UE) 2019/881;

26 *bis quater*) «proveedor de servicios administrados»: toda entidad que preste servicios de redes, aplicaciones, infraestructura y seguridad por medio de una gestión, soporte y administración activa permanentes y habituales en las instalaciones del usuario, en el centro de datos de su proveedor de servicios de administrados (alojamiento) o en el centro de datos de un tercero;

26 *bis quinquies*) «proveedor de servicios de seguridad administrados»: toda entidad que se encargue de la supervisión y la administración externalizadas de dispositivos y sistemas de seguridad. Entre los servicios normalmente prestados figuran los cortafuegos administrados, la detección de intrusiones, las redes virtuales privadas, la exploración de vulnerabilidades y los servicios antivirus.

También incluye el uso de centros de operaciones de seguridad de alta disponibilidad (ya sea desde sus propias instalaciones o desde otros proveedores de centros de datos) para prestar servicios ininterrumpidos concebidos para reducir el número de personal operativo de seguridad que una empresa necesita contratar, formar y conservar para mantener un nivel de seguridad aceptable.

CAPÍTULO II

Marcos reglamentarios de ciberseguridad coordinados

Artículo 5

Estrategia nacional de ciberseguridad

1. Cada Estado miembro adoptará una estrategia nacional de ciberseguridad en la que se establecerán los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de ciberseguridad. La estrategia nacional de ciberseguridad incluirá, en particular, los aspectos siguientes:

   a) […] los objetivos y las prioridades de la estrategia de ciberseguridad de los Estados miembros;

   b) un marco de gobernanza para lograr dichos objetivos y prioridades, incluidas las políticas a que se refiere el apartado 2 y las funciones y responsabilidades de las diversas autoridades y actores que participen en la ejecución de la estrategia […];

   c) […] **directrices** para determinar los activos pertinentes y **evaluar** los riesgos de ciberseguridad en ese Estado miembro;

   d) una determinación de las medidas para garantizar la preparación, respuesta y recuperación frente a incidentes, incluida la cooperación entre los sectores público y privado;

   e) […]

f) un marco de actuación para la coordinación reforzada entre las autoridades competentes en virtud de la presente Directiva y la Directiva (UE) XXXX/XXXX del Parlamento Europeo y del Consejo [Directiva sobre la resiliencia de las entidades críticas][38] a efectos del intercambio de información sobre los **riesgos de ciberseguridad,** […] las ciberamenazas **y los ciberincidentes, así como sobre los riesgos, amenazas e incidentes no cibernéticos,** y el ejercicio de las tareas de supervisión, **según proceda**;

f *bis*) un marco de actuación para la coordinación y la cooperación entre las autoridades competentes en virtud de la presente Directiva y las autoridades competentes designadas en virtud de la legislación sectorial.

2. En el marco de la estrategia nacional de ciberseguridad, los Estados miembros adoptarán, en particular, las siguientes políticas:

a) una política para abordar la ciberseguridad en la cadena de suministro de productos y servicios de TIC utilizados por las entidades […] para la prestación de sus servicios;

b) **una política** […] relativa a la inclusión y especificación de los requisitos en materia de ciberseguridad aplicables a los productos y servicios de TIC en la contratación pública, **en particular la certificación de la ciberseguridad**;

c) una política **relativa a la gestión de las vulnerabilidades, que promueva y facilite la** […] divulgación coordinada **y voluntaria** de las vulnerabilidades en el sentido del artículo 6**, apartado 1**;

d) una política orientada a mantener la disponibilidad general**,** […] la integridad **y la confidencialidad** del núcleo público de la internet abierta;

e) una política sobre la promoción y el desarrollo de iniciativas de **educación y formación,** desarrollo de capacidades, concienciación, e investigación y desarrollo en materia de ciberseguridad;

---

38 *[insértese el título completo y la referencia de publicación en el DO cuando se conozcan]*.

f) una política destinada a prestar apoyo a las instituciones académicas y de investigación para que desarrollen herramientas de ciberseguridad e infraestructuras de red seguras;

g) una política, los procedimientos pertinentes y las herramientas apropiadas para compartir información en apoyo del intercambio voluntario de información sobre ciberseguridad entre las empresas, con arreglo al Derecho de la Unión;

h) una política que atienda a las necesidades específicas de las pymes, especialmente de las excluidas del ámbito de aplicación de la presente Directiva, por lo que respecta a orientaciones y apoyo para mejorar su resiliencia frente a las ciberamenazas […].

3. Los Estados miembros notificarán sus estrategias nacionales de ciberseguridad a la Comisión en el plazo de tres meses a partir de su adopción. **Cuando notifiquen sus estrategias,** los Estados miembros podrán **excluir elementos de la estrategia que estén relacionados con** […] la seguridad nacional.

4. Los Estados miembros evaluarán sus estrategias nacionales de ciberseguridad de forma periódica y al menos cada […] **cinco** años en función de unos indicadores de rendimiento clave, y las modificarán cuando proceda. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) prestará asistencia a los Estados miembros, cuando así lo soliciten, a la hora de elaborar una estrategia nacional y los indicadores de rendimiento clave para su evaluación.

Artículo 6

Divulgación coordinada de las vulnerabilidades y Registro Europeo de Vulnerabilidades

1. Cada Estado miembros designará a uno de sus CSIRT referidos en el artículo 9 como coordinador a efectos de la divulgación coordinada de las vulnerabilidades. El CSIRT designado ejercerá de intermediario de confianza y facilitará, cuando sea necesario, la interacción entre la entidad notificante**, la posible parte vulnerable** y el fabricante o proveedor de productos o servicios de TIC. **Cualquier persona física o jurídica puede notificar, incluso anónimamente, una vulnerabilidad en el sentido de lo dispuesto en el artículo 4, punto 8), al CSIRT designado. El CSIRT designado velará por que la notificación se tramite diligentemente y por que la identidad de la persona que haya notificado la vulnerabilidad sea confidencial.** Cuando la vulnerabilidad notificada […] **pueda repercutir significativamente en entidades de más de un Estado miembro**, el CSIRT designado de cada Estado miembro afectado cooperará**, cuando proceda,** con **los demás CSIRT designados en el marco de** la red de CSIRT.

2. La ENISA desarrollará y mantendrá un Registro Europeo de Vulnerabilidades**, en consulta con el Grupo de Cooperación**. Para ello, la Agencia establecerá y mantendrá los sistemas de información, las políticas y los procedimientos apropiados con vistas, en particular, a permitir que las entidades importantes y esenciales y sus proveedores de redes y sistemas de información divulguen y registren**, de forma voluntaria,** vulnerabilidades **de dominio público** presentes en los productos o servicios de TIC, así como a facilitar a todas las partes interesadas acceso a la información sobre vulnerabilidades que figura en el registro. Concretamente, el registro contendrá información que describa la vulnerabilidad, los productos o servicios de TIC afectados y la gravedad de la vulnerabilidad por lo que respecta a las circunstancias en que puede explotarse, la disponibilidad de los parches de seguridad asociados y, a falta de ellos, orientaciones **de las autoridades nacionales competentes o de los CSIRT** dirigidas a los usuarios de productos y servicios vulnerables sobre la forma de reducir los riesgos derivados de las vulnerabilidades reveladas. **La ENISA garantizará que el Registro Europeo de Vulnerabilidades use una infraestructura de comunicación e información segura y resiliente.**

Artículo 7

Marcos nacionales de gestión de crisis de ciberseguridad

1. Cada Estado miembro designará una o varias autoridades competentes responsables de la gestión de incidentes y crisis **de ciberseguridad** a gran escala. Los Estados miembros velarán por que las autoridades competentes dispongan de los recursos adecuados para ejercer las tareas que les sean asignadas de forma efectiva y eficiente. **Los Estados miembros velarán por la coherencia con los marcos vigentes de gestión general de crisis.**

2. Cada Estado miembro determinará las capacidades, los activos y los procedimientos que se pueden desplegar en caso de que se produzca una crisis a los efectos de la presente Directiva.

3. Cada Estado miembro adoptará un plan nacional de respuesta a incidentes y crisis de ciberseguridad en el que se fijen los objetivos y las modalidades de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. El plan establecerá, en particular, los siguientes aspectos:

   a) los objetivos de las medidas y actividades nacionales en materia de preparación;

   b) las tareas y responsabilidades de las autoridades nacionales competentes;

   c) los procedimientos de gestión de crisis de ciberseguridad**, incluida su integración en el marco nacional general de gestión de crisis,** y los canales para el intercambio de información;

   d) las medidas de preparación, incluidos ejercicios y actividades de formación periódicos;

   e) las partes […] pertinentes, tanto públicas como privadas, y la infraestructura implicada;

   f) los procedimientos y mecanismos nacionales entre las autoridades y los organismos nacionales pertinentes para garantizar la participación efectiva del Estado miembro en la gestión coordinada de incidentes y crisis de ciberseguridad a gran escala a nivel de la Unión y el respaldo de ella.

4. Los Estados miembros […] **informarán** a la Comisión **de** la designación de sus autoridades competentes referidas en el apartado 1 y proporcionarán **información pertinente relativa a los requisitos del apartado 3 del presente artículo** sobre sus planes nacionales de respuesta a incidentes y crisis de ciberseguridad […] en el plazo de tres meses a partir de tal designación y la adopción de dichos planes. Los Estados miembros podrán excluir información específica […] cuando y en la medida en que sea […] necesario para su seguridad nacional**, la seguridad pública o la defensa**.

Artículo 8

Autoridades nacionales competentes y puntos de contacto únicos

1. Cada Estado miembro designará una o más autoridades competentes encargadas de la ciberseguridad y de las tareas de supervisión a que se refiere el capítulo VI de la presente Directiva. Los Estados miembros podrán designar a tales efectos una autoridad o autoridades existentes.

2. Las autoridades competentes a que se refiere el apartado 1 supervisarán la aplicación de la presente Directiva a escala nacional.

3. Cada Estado miembro designará un punto de contacto único en materia de ciberseguridad (en lo sucesivo, «punto de contacto único»). Si un Estado miembro designa únicamente una autoridad competente, dicha autoridad también será el punto de contacto único correspondiente a dicho Estado miembro.

4. Cada punto de contacto único ejercerá una función de enlace para garantizar la cooperación transfronteriza de las autoridades de su Estado miembro con las autoridades competentes en otros Estados miembros, así como para garantizar la cooperación intersectorial con otras autoridades nacionales competentes dentro de su Estado miembro.

5. Los Estados miembros velarán por que las autoridades competentes a que se refiere el apartado 1 y los puntos de contacto únicos dispongan de recursos adecuados para ejercer las funciones que les sean 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 a que se refiere el artículo 12.

6. Los Estados miembros notificarán sin dilación indebida a la Comisión la autoridad competente a que se refiere el apartado 1 y el punto de contacto único contemplado en el apartado 3 que hayan designado, sus tareas y cualquier cambio posterior que se introduzca. Cada Estado miembro hará pública su designación. 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 cumplirán los requisitos establecidos en el artículo 10, apartado 1, que cubran al menos los sectores, subsectores o entidades que figuran en los anexos I y II y se responsabilicen de la gestión de incidentes de conformidad con un procedimiento claramente definido. Podrá crearse un CSIRT en el marco de una autoridad competente a que se refiere el artículo 8.

2. Los Estados miembros velarán por que cada CSIRT disponga de los recursos adecuados para llevar a cabo eficazmente sus tareas, tal como se establece en el artículo 10, apartado 2. **En el desempeño de sus tareas, los CSIRT podrán priorizar la prestación de determinados servicios a las entidades con arreglo a un planteamiento basado en el riesgo.**

3. Los Estados miembros velarán por que cada CSIRT tenga a su disposición una infraestructura de comunicación e información apropiada, segura y resiliente para intercambiar información con las entidades esenciales e importantes y otras partes interesadas pertinentes. Para ello, los Estados miembros se asegurarán de que los CSIRT contribuyan al despliegue de herramientas seguras para el intercambio de información.

4. Los CSIRT cooperarán y, cuando proceda, intercambiarán información pertinente de conformidad con el artículo 26 con comunidades sectoriales o intersectoriales de entidades esenciales e importantes de confianza.

5. Los CSIRT participarán en las rondas de **aprendizaje** entre iguales que se organicen con arreglo al artículo 16.

6. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT a que se refiere el artículo 13.

7. Los Estados miembros comunicarán a la Comisión sin demora indebida los CSIRT designados de conformidad con el apartado 1, el CSIRT coordinador designado con arreglo al artículo 6, apartado 1, y sus respectivas tareas desempeñadas en relación con las entidades contempladas en los anexos I y II.

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

Artículo 10

Obligaciones y tareas de los CSIRT

1. Los CSIRT cumplirán las siguientes obligaciones:

   a) los CSIRT garantizarán una gran disponibilidad de sus […] **canales** de comunicación evitando los puntos únicos de fallo y contarán con varios medios para ser contactados y contactar con otros en todo momento. Los CSIRT especificarán claramente los canales de comunicación y los darán a conocer a 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) los CSIRT estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes, en particular, con el fin de facilitar la efectividad y eficiencia de los traspasos;

d) los CSIRT contarán con personal suficiente para garantizar su disponibilidad en todo momento;

e) los CSIRT estarán dotados de sistemas redundantes y espacios de trabajo de reserva para garantizar la continuidad de sus servicios;

f) los CSIRT podrán participar en redes de cooperación internacional.

2. Las tareas de los CSIRT serán las siguientes:

a) supervisar las ciberamenazas, las vulnerabilidades y los incidentes a escala nacional;

b) difundir alertas tempranas, alertas, avisos e información sobre las ciberamenazas, las vulnerabilidades y los incidentes entre las entidades esenciales e importantes**, las autoridades competentes y** otras partes interesadas pertinentes;

c) responder a incidentes;

d) recopilar y analizar datos forenses y efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación en materia de ciberseguridad;

e) llevar a cabo […] una exploración proactiva de las redes y los sistemas de información […] **para detectar vulnerabilidades que podrían tener un efecto significativo, siempre que dicha exploración no suponga acceder sin autorización a las redes y los sistemas de información ni tenga un efecto negativo en su funcionamiento, salvo que la entidad haya dado su consentimiento para ello;**

f) participar en la red de CSIRT y prestar asistencia mutua**, según sus capacidades y competencias,** a otros miembros de la red cuando la soliciten;

f *bis*) en su caso, desempeñar la función de coordinador a los efectos del procedimiento de divulgación coordinada de las vulnerabilidades previsto en el artículo 6, apartado 1, lo que incluirá, en particular, facilitar la interacción entre las entidades notificantes, la posible parte vulnerable y el fabricante o proveedor de productos o servicios de TIC en los casos en que sea necesario; identificar y contactar a las entidades afectadas; prestar asistencia a las entidades notificantes; negociar los plazos de divulgación, y gestionar las vulnerabilidades que afecten a varias organizaciones (divulgación coordinada de vulnerabilidades con múltiples interesados).

3. Los CSIRT establecerán relaciones de cooperación con actores pertinentes del sector privado, con vistas a mejorar la consecución de los objetivos de la Directiva.

3 *bis*. Los CSIRT podrán entablar relaciones de cooperación con los CSIRT nacionales de terceros países. En el marco de dicha cooperación, podrán intercambiar información pertinente, incluidos datos personales de conformidad con la legislación de la Unión en materia de protección de datos.

4. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas, sistemas de clasificación y taxonomías en relación con los siguientes aspectos:

a) los procedimientos de gestión de incidentes;

b) la gestión de crisis de ciberseguridad;

c) la divulgación coordinada de las vulnerabilidades.

Artículo 11

Cooperación a escala nacional

1. Cuando sean distintos, las autoridades competentes referidas en el artículo 8, el punto de contacto único y los CSIRT del mismo Estado miembro cooperarán entre sí respecto al cumplimiento de las obligaciones establecidas en la presente Directiva.

2. Los Estados miembros velarán por que sus autoridades competentes o sus CSIRT reciban las notificaciones sobre los incidentes y los cuasiincidentes y ciberamenazas significativos presentadas en el marco de la presente Directiva. Cuando un Estado miembro decida que sus CSIRT no recibirán dichas notificaciones, se dará a estos últimos, en la medida necesaria para que lleven a cabo sus tareas, el acceso a los datos sobre incidentes notificados por las entidades esenciales o importantes, con arreglo al artículo 20.

3. Cada Estado miembro velará por que sus autoridades competentes o los CSIRT informen a su punto de contacto único sobre las notificaciones de incidentes, y cuasiincidentes y ciberamenazas significativos presentadas en el marco de la presente Directiva.

4. En la medida necesaria para cumplir de manera efectiva las tareas y obligaciones establecidas en la presente Directiva, los Estados miembros garantizarán una cooperación apropiada, dentro del Estado miembro, entre las autoridades competentes**, los CSIRT**, los puntos de contacto únicos, las autoridades policiales y las autoridades de protección de datos, así como las autoridades **competentes designadas** […] con arreglo a la Directiva (UE) XXXX/XXXX [Directiva sobre la Resiliencia de las Entidades Críticas]**, las autoridades competentes en virtud del Reglamento de Ejecución 2019/1583 de la Comisión, las autoridades nacionales de reglamentación designadas con arreglo a la Directiva (UE) 2018/1972, las autoridades nacionales designadas con arreglo al artículo 17 del Reglamento (UE) n.º 910/2014,** y las autoridades financieras nacionales designadas de conformidad con el Reglamento (UE) XXXX/XXXX del Parlamento Europeo y del Consejo [Reglamento sobre la Resiliencia Operativa Digital del Sector Financiero]**, así como las autoridades competentes designadas en virtud de otros actos sectoriales de la Unión**.

5. Los Estados miembros velarán por que sus autoridades competentes **en virtud de la presente Directiva y las autoridades competentes designadas con arreglo a la Directiva (UE) XXXX/XXXX [Directiva sobre la Resiliencia de las Entidades Críticas] intercambien** […] periódicamente información […] sobre **la determinación de entidades críticas,** los riesgos de ciberseguridad, las ciberamenazas y los **ciber**incidentes**, así como los riesgos, las amenazas y los incidentes no cibernéticos**, que afecten a entidades esenciales identificadas como críticas, **[**o como entidades equivalentes a entidades críticas,**]** con arreglo a la Directiva (UE) XXXX/XXXX [Directiva sobre la Resiliencia de las Entidades Críticas], así como las medidas adoptadas […] en respuesta a estos riesgos e incidentes. **Los Estados miembros también velarán por que las autoridades competentes en virtud de la presente Directiva […] y las autoridades competentes designadas en virtud del Reglamento XXXX/XXXX [Reglamento sobre la Resiliencia Operativa Digital del Sector Financiero], la Directiva 2018/1972 y el Reglamento (UE) 910/2014 intercambien información pertinente de forma periódica.**

Por lo que se refiere a los proveedores de servicios de confianza y […] en particular […] en los casos en que esa función de supervisión en virtud de la presente Directiva se asigne a un organismo distinto de los organismos de supervisión designados de conformidad con el Reglamento (UE) 910/2014, las autoridades nacionales competentes en virtud de la presente Directiva cooperarán estrechamente, en el momento oportuno, intercambiando información pertinente para garantizar la supervisión efectiva y el cumplimiento por parte de los proveedores de servicios de confianza de los requisitos establecidos en la presente Directiva y en el Reglamento [XXXX/XXXX] **y, cuando proceda, la autoridad nacional competente en virtud de la presente Directiva informará sin demora indebida al organismo de supervisión del Reglamento eIDAS de cualquier ciberamenaza o ciberincidente significativo notificado que repercuta en los servicios de confianza**.

5 *bis*. A fin de […] simplificar la notificación de incidentes, los Estados miembros pueden establecer un punto de entrada único para todas las notificaciones obligatorias exigidas en virtud de la presente Directiva, del Reglamento (UE) 2016/679 y de la Directiva 2002/58/CE, en su caso. Los Estados miembros también podrán utilizar el punto de entrada único para las notificaciones exigidas en virtud de otros actos sectoriales de la Unión. El punto de entrada único no afectará a la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE, en particular por lo que respecta a las autoridades de control independientes.

CAPÍTULO III

*Cooperación **de la UE***

Artículo 12

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 para fortalecer la confianza y la colaboración** […].

2. El Grupo de Cooperación llevará a cabo sus tareas con arreglo a los programas de trabajo bienales a que se refiere el apartado 6.

3. El Grupo de Cooperación estará formado por representantes de los Estados miembros, la Comisión y la ENISA. El Servicio Europeo de Acción Exterior participará en las actividades del Grupo de Cooperación en calidad de observador. Las Autoridades Europeas de Supervisión (AES) **y las autoridades competentes designadas con arreglo al Reglamento (UE) XXXX/XXXX [Reglamento sobre la Resiliencia Operativa Digital del Sector Financiero]** […] podrán participar en las actividades del Grupo de Cooperación **de conformidad con el artículo 42, apartado 1, del Reglamento (UE) XXXX/XXXX [el Reglamento sobre la Resiliencia Operativa Digital del Sector Financiero].**

   Cuando proceda, el Grupo de Cooperación podrá invitar a representantes de las partes interesadas pertinentes a que participen en su labor.

   La Comisión se hará cargo de la secretaría.

4. El Grupo de Cooperación llevará a cabo las siguientes tareas:

   a) proporcionar orientación a las autoridades competentes en relación con la transposición y aplicación de la presente Directiva**;**

   a *bis*) Proporcionar orientación en relación con el desarrollo y la ejecución de políticas sobre divulgación coordinada de vulnerabilidades a que se refieren el artículo 5, apartado 2, letra c), y el artículo 6, apartado 1;

b) intercambiar buenas prácticas e información en relación con la aplicación de la presente Directiva, también por lo que respecta a las ciberamenazas, los incidentes, las vulnerabilidades, los cuasiincidentes, las iniciativas de concienciación, las formaciones, los ejercicios y las habilidades, el desarrollo de capacidades, así como las normas y especificaciones técnicas;

c) intercambiar recomendaciones y cooperar con la Comisión en iniciativas políticas sobre aspectos emergentes de la ciberseguridad;

d) intercambiar recomendaciones y cooperar con la Comisión en la redacción de los actos […] de ejecución que adopte en virtud de la presente Directiva;

e) intercambiar buenas prácticas e información con las instituciones, los órganos y los organismos de la Unión pertinentes;

e *bis*) intercambiar puntos de vista sobre la aplicación de la legislación sectorial con aspectos de ciberseguridad;

f) analizar los informes sobre […] **las rondas aprendizaje** entre iguales a que se refiere el artículo 16, apartado 7;

g) analizar […] **las experiencias** de las actividades conjuntas de supervisión en casos transfronterizos, tal como se contempla en el artículo 34;

h) proporcionar orientación estratégica a la red de CSIRT **y a la red de funcionarios de enlace nacionales para la gestión de cibercrisis EU-CyCLONe** sobre cuestiones emergentes específicas;

h *bis*)intercambiar puntos de vista sobre el seguimiento en las políticas de incidentes de ciberseguridad a gran escala sobre la base de la experiencia adquirida de la red de CSIRT y EU-CyCLONe;

i) contribuir a las capacidades de ciberseguridad de toda la Unión facilitando el intercambio de funcionarios nacionales a través de un programa de desarrollo de capacidades en el que participe el personal de las autoridades competentes o los CSIRT de los Estados miembros;

j) organizar reuniones conjuntas periódicas con las partes interesadas privadas pertinentes de toda la Unión para tratar las actividades realizadas por el Grupo y recabar apreciaciones sobre los desafíos políticos emergentes;

k) debatir sobre las labores realizadas en relación con los ejercicios de ciberseguridad, incluida la labor efectuada por la ENISA**;**

k *bis*)establecer el mecanismo de aprendizaje entre iguales de conformidad con el artículo 16 de la presente Directiva.

5. El Grupo de Cooperación podrá solicitar a la red de CSIRT un informe técnico sobre temas concretos.

6. A más tardar el …[veinticuatro meses después de la fecha de 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 alcanzar sus objetivos y llevar a cabo sus tareas. El calendario del primer programa adoptado en virtud de la presente Directiva se adecuará al del último programa adoptado con arreglo a la Directiva (UE) 2016/1148.

7. La Comisión podrá adoptar 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 37, apartado 2.

8. El Grupo de Cooperación se reunirá periódicamente, y por lo menos una vez al año, con el Grupo de resiliencia de las entidades críticas establecido en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] para promover la cooperación estratégica y **facilitar** el intercambio de información.

Artículo 13

Red de CSIRT

1. Con vistas a contribuir al refuerzo de la confianza y la seguridad y la promoción de una cooperación operativa rápida y eficaz entre los Estados miembros, se establece una red de CSIRT nacionales.

2. La red de CSIRT estará formada por representantes de los CSIRT de los Estados miembros **designados de conformidad con el artículo 9** y el CERT-UE. 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 llevará a cabo las siguientes tareas:

   a) intercambiar información sobre las capacidades de los CSIRT;

   b) intercambiar información pertinente sobre los incidentes, los cuasiincidentes, las ciberamenazas, los riesgos y las vulnerabilidades;

b *bis*) intercambiar información sobre publicaciones y recomendaciones en materia en materia de ciberseguridad;

b *ter*) compartir soluciones técnicas que faciliten la gestión técnica de los incidentes;

b *quater*) intercambiar buenas prácticas, instrumentos y procesos en relación con las tareas de los CSIRT;

c) a instancias de un […] **miembro** de la red de CSIRT que pueda verse afectado por un incidente, intercambiar y debatir información relacionada con ese incidente y las ciberamenazas, los riesgos y las vulnerabilidades asociados;

d) a instancias de un […] **miembro** de la red de CSIRT, debatir y, cuando sea posible, aplicar una respuesta coordinada a un incidente que se haya detectado dentro del ámbito de competencias de ese Estado miembro;

e) prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos con arreglo a la presente Directiva;

f) cooperar**, intercambiar buenas prácticas** y prestar asistencia a los CSIRT designados a que se refiere el artículo 6 por lo que respecta a la gestión de la divulgación coordinada de las vulnerabilidades […] que afecten a varios fabricantes o proveedores de productos, servicios y procesos de TIC establecidos en distintos Estados miembros;

g) debatir y determinar más formas de cooperación operativa, incluidas las relacionadas con:

i) las categorías de ciberamenazas e incidentes,

ii) las alertas tempranas,

iii) la asistencia mutua,

iv) los principios y las modalidades de coordinación en respuesta a riesgos e incidentes transfronterizos,

v) la contribución al plan nacional de respuesta a incidentes y crisis de ciberseguridad a que se refiere el artículo 7, apartado 3, **a petición de un Estado miembro**;

h) informar al Grupo de Cooperación sobre sus actividades y sobre las formas adicionales de cooperación operativa sobre las que se haya discutido conforme a la letra g), y solicitar, cuando sea necesario, directrices a este respecto;

i) hacer balance de los ejercicios de ciberseguridad, también de los organizados por la ENISA;

j) a instancias de un CSIRT determinado, analizar las capacidades y la preparación de dicho CSIRT;

k) cooperar e intercambiar información con los centros de operaciones de seguridad (COS) regionales y a escala de la Unión para mejorar el conocimiento común de la situación relativa a los incidentes y las amenazas en toda la Unión;

l) analizar los informes sobre […] **las rondas de aprendizaje** entre iguales a que se refiere el artículo 16, apartado 7;

m) publicar directrices para facilitar la convergencia de las 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 a que se refiere el artículo 35, a más tardar [veinticuatro meses después de la fecha de entrada en vigor de la presente Directiva], y cada dos años a partir de entonces, la red de CSIRT evaluará los progresos realizados en el ámbito de la cooperación operativa y elaborará un informe. Concretamente, el informe extraerá conclusiones sobre los resultados de […] las **rondas de aprendizaje** entre iguales a que se refiere el artículo 16 realizad**a**s en relación con los CSIRT nacionales, en particular las conclusiones y recomendaciones, practicadas con arreglo al presente artículo. Dicho informe también se enviará al Grupo de Cooperación.

5. La red de CSIRT adoptará su reglamento interno.

6. La red de CSIRT cooperará con EU-CyCLONe sobre la base de disposiciones de procedimiento acordadas.

Artículo 14

Red europea de funcionarios de enlace nacionales para la gestión de cibercrisis (EU-CyCLONe)

1. De cara a respaldar la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio regular de información entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión, se crea la red de funcionarios de enlace nacionales para la gestión de cibercrisis EU-CyCLONe).

2. EU-CyCLONe estará formada por representantes de las autoridades de gestión de crisis **cibernéticas** de los Estados miembros designadas con arreglo al artículo 7 […]. **La Comisión participará en las actividades de la red en calidad de observador.** La ENISA se hará cargo de la secretaría de la red y promoverá el intercambio seguro de información**, y también facilitará las herramientas necesarias para apoyar la cooperación entre los Estados miembros garantizando un intercambio seguro de la información.**

Cuando proceda, EU-CyCLONe podrá invitar a representantes de las partes interesadas pertinentes a que participen en su labor.

3. Las tareas de EU-CyCLONe serán las siguientes:

a) incrementar el nivel de preparación para la gestión de incidentes y crisis **de ciberseguridad** a gran escala;

b) desarrollar una conciencia situacional conjunta […] para incidentes y crisis **de ciberseguridad** a gran escala;

b *bis*) evaluar las consecuencias y las repercusiones de los incidentes pertinentes de ciberseguridad a gran escala y proponer posibles medidas de mitigación;

c) coordinar la gestión de incidentes y crisis **de ciberseguridad** a gran escala y contribuir a la toma de decisiones a nivel político en relación con tales incidentes y crisis;

d) **a petición de un Estado miembro,** debatir **sus** planes de respuesta nacionales a incidentes y **crisis** de ciberseguridad a que se refiere el artículo 7**, apartado 3** […]**;**[…]

4. EU-CyCLONe adoptará su reglamento interno.

5. EU-CyCLONe informará periódicamente al Grupo de Cooperación de **la gestión de los incidentes y crisis de ciberseguridad a gran escala** […], con atención especial a sus […] repercusiones para las entidades esenciales e importantes.

6. EU-CyCLONe cooperará con la red de CSIRT sobre la base de disposiciones de procedimiento acordadas.

7. EU-CyCLONe presentará al Parlamento Europeo y al Consejo un informe de evaluación de sus trabajos a más tardar [veinticuatro meses después de la fecha de entrada en vigor de la presente Directiva].

Artículo 14 **bis**

Cooperación internacional

La Unión podrá celebrar, cuando corresponda y 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, la red de CSIRT y EU-CyCLONe, de conformidad con la legislación de la Unión en materia de protección de datos.

Artículo 15

Informe sobre la situación de la ciberseguridad en la Unión

1. La ENISA publicará, en cooperación con la Comisión **y el Grupo de Cooperación**, un informe bienal sobre la situación de la ciberseguridad en la Unión. **En particular, e**l informe deberá […] incluir […] la siguiente información:

a *bis*) una evaluación de los riesgos de ciberseguridad a escala de la Unión, teniendo en cuenta el panorama de amenazas;

a) […] **una evaluación del** desarrollo de las capacidades de ciberseguridad en **los** sector**es** público y privado en toda la Unión;

b) […]

c) **una evaluación agregada basada en indicadores cuantitativos y cualitativos** en materia de ciberseguridad […] que proporcione una […] **visión general** del nivel de madurez e las capacidades de ciberseguridad**, incluidas las capacidades sectoriales**.

2. El informe incluirá recomendaciones políticas concretas para incrementar el nivel de ciberseguridad en toda la Unión y un resumen de las conclusiones correspondientes al período de que se trate de los informes sobre la situación técnica de la ciberseguridad en la UE publicados por la ENISA de conformidad con el artículo 7, apartado 6, del Reglamento (UE) 2019/881.

Artículo 16

Aprendizaje entre iguales

1. **Con vistas a reforzar la confianza recíproca, alcanzar un nivel común elevado de ciberseguridad y reforzar las capacidades y políticas en materia de ciberseguridad de los Estados miembros necesarias para la aplicación efectiva de la presente Directiva, e**[…]l **Grupo de Cooperación** […] establecerá, **con el apoyo de la Comisión y** tras consultar a la […] ENISA**, y, cuando proceda, a la red de CSIRT,** y a más tardar **veinticuatro […]** meses después de la entrada en vigor de la presente Directiva, la metodología […] **para un sistema de aprendizaje entre iguales objetivo, no discriminatorio y justo** […] **en relación con la aplicación de la presente Directiva** por los Estados miembros. **La participación en el aprendizaje entre iguales es voluntaria.** El **sistema consistirá en rondas de evaluación** […] realizadas por expertos […] en ciberseguridad procedentes de los Estados miembros […] y abarcarán […] **uno o varios de** los siguientes aspectos:

   i) la […] aplicación de los requisitos de gestión de riesgos de ciberseguridad y las obligaciones de notificación a que se refieren los artículos 18 y 20;

   ii) las […] capacidades, incluidos los […] recursos disponibles, y el […] ejercicio de las tareas de las autoridades nacionales competentes **a que se refiere el artículo 8 y los CSIRT a que se refiere el artículo 9**;

[…]

i**ii** […]) la […] **aplicación** de la asistencia mutua a que se refiere el artículo 34;

iv) la […] **aplicación** del marco para el intercambio de información a que se refiere el artículo 26 […].

2. **Los criterios en los que se basen los Estados miembros para la designación de los expertos admisibles para participar en las rondas de aprendizaje entre iguales deberán ser** […] objetivos, no discriminatorios, justos y transparentes […] **y deberán incluirse en la metodología a que se refiere el apartado 1**. La ENISA y la Comisión **podrán** designar […] expertos para que participen en las […] **rondas de aprendizaje entre iguales** en calidad de observadores. […]

3. […].

3 *bis*. Antes del inicio de las rondas de aprendizaje entre iguales, los Estados miembros podrán llevar a cabo una autoevaluación de los aspectos cubiertos por esa ronda concreta de aprendizaje entre iguales y facilitar dicha autoevaluación a los expertos designados a que se refiere el apartado 2.

4. […] **Las rondas de aprendizaje entre iguales podrán conllevar** […] visitas *in situ* presenciales o virtuales e intercambios a distancia. En consideración del principio de buena cooperación, los Estados miembros […] **que participen en el aprendizaje entre iguales** facilitarán a los expertos designados la información […] necesaria para la evaluación […]**, sin perjuicio de las leyes nacionales o de la Unión relativas a la protección de información confidencial o clasificada o a la salvaguardia de las funciones esenciales del Estado, como la seguridad nacional.** Cualquier información obtenida a través del proceso de […] **aprendizaje entre iguales** se utilizará exclusivamente para tal finalidad. Los expertos que participen en […] **el aprendizaje entre iguales** no divulgarán a terceros ninguna información sensible o confidencial obtenida en […] **este contexto**. **El Estado miembro que participe en el aprendizaje entre iguales podrá oponerse a la designación de expertos concretos por motivos debidamente justificados comunicados al Grupo de Cooperación.**

5. Una vez **hayan sido objeto de una ronda de aprendizaje entre iguales** […], los mismos aspectos no podrán ser objeto de nuevas rondas de […]**aprendizaje entre iguales** […] **efectuadas por los** Estados miembros **participantes** durante los […] **cuatro** […] años siguientes a la conclusión de la **citada**[…] **ronda de aprendizaje entre iguales**, **a menos que el Estado miembro afectado lo solicite o acepte una propuesta en este sentido presentada** […] por el **Grupo de Cooperación […]**.

6. […]

7. Los expertos que participen en […] **rondas de aprendizaje entre iguales** elaborarán informes sobre las constataciones y conclusiones de las […] **evaluaciones**. **Los Estados miembros podrán formular observaciones sobre sus respectivos proyectos de informe, que se adjuntarán al informe.** Los informes **finales** deberán presentarse al […] Grupo de Cooperación […] **y los Estados miembros podrán optar por hacer públicos sus respectivos informes.**

CAPÍTULO IV

Obligaciones de gestión de riesgos de ciberseguridad y notificación

SECCIÓN I

Gestión de riesgos de ciberseguridad y notificación

Artículo 17

Gobernanza

1. Los Estados miembros velarán por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas de gestión de los riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 18, supervisen su puesta en práctica y […] **puedan ser consideradas responsables** por el incumplimiento de las obligaciones recogidas en el presente artículo por parte de las entidades.

   La aplicación del presente apartado se entenderá sin perjuicio de la legislación nacional de los Estados miembros relativa a las normas sobre responsabilidad en las instituciones públicas, así como a la responsabilidad de los funcionarios públicos y los cargos electos y designados.

2. Los Estados miembros garantizarán que los **miembros del órgano de dirección** […] **tengan la obligación de** asistir periódicamente a formaciones […] para adquirir conocimientos y destrezas suficientes que permitan comprender y evaluar los riesgos de ciberseguridad y las prácticas de gestión y su impacto en las operaciones de la entidad.

Artículo 18

Medidas para la gestión de riesgos de ciberseguridad

1***bis*. La presente Directiva aplica un enfoque que abarca todos los peligros y que incluye la protección de las redes y los sistemas de información y su entorno físico de cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por redes y sistemas de información o accesibles a través de ellos.**

1. Los Estados miembros velarán por que las entidades esenciales e importantes 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 dichas entidades para la prestación de sus servicios. Habida cuenta de la situación **y del coste de ejecución**, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado. **Al evaluar la proporcionalidad de las medidas, se tendrá debidamente en cuenta el grado de exposición a los riesgos de la entidad, su tamaño, la posibilidad de que se produzcan incidentes y su gravedad. Teniendo en cuenta el nivel y el tipo de riesgo para la sociedad en caso de que ocurran incidentes que afecten a entidades importantes o esenciales, las medidas para la gestión de riesgos de ciberseguridad que se impongan a entidades importantes pueden ser menos estrictas que las que se impongan a entidades esenciales.**

2. Las medidas a que se hace referencia en el apartado 1 incluirán, al menos, los siguientes elementos:

a) las políticas de seguridad de los sistemas de información y análisis de riesgos;

b) la gestión de incidentes (prevención, detección, […] respuesta **y recuperación frente a** […] incidentes);

c) la continuidad de las actividades y la gestión de crisis;

d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios **directos**, como, por ejemplo, proveedores de servicios de almacenamiento y tratamiento de datos o servicios de seguridad administrada;

e) la seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluidas la gestión y divulgación de las vulnerabilidades;

f) las políticas y los procedimientos […] para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;

g) **la política sobre** la utilización de criptografía y cifrado;

g *bis*) la seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.

3. Los Estados miembros velarán por que, a la hora de estudiar las medidas apropiadas a que se refiere el apartado 2, letra d), las entidades […] **tengan la obligación de** tener en cuenta las vulnerabilidades específicas de cada proveedor y prestador de servicios **directo** y la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro. **Los Estados miembros también velarán por que, a la hora de estudiar las medidas apropiadas a que se refiere el apartado 2, letra d), las entidades tengan la obligación de tener en cuenta los resultados de las evaluaciones coordinadas de los riesgos realizadas de conformidad con el artículo 19, apartado 1.**

4. Los Estados miembros se asegurarán de que, cuando una entidad constate, respectivamente, que sus servicios o cometidos no se ajustan a los requisitos establecidos en el apartado 2, esta adopte, sin demora indebida, todas las medidas correctoras necesarias para que el servicio en cuestión cumpla dichos requisitos.

5. La Comisión podrá adoptar actos de ejecución para establecer las modalidades técnicas y metodológicas, **así como las especificidades sectoriales,** cuando sea necesario, de los elementos a que se refiere el apartado 2 **del presente artículo**. **La Comisión adoptará a más tardar [dieciocho meses después de la entrada en vigor de la presente Directiva] actos de ejecución para establecer las modalidades técnicas y metodológicas para las entidades a que se refiere el artículo 24, apartado 1, y los prestadores de servicios de confianza a que se refiere el punto 8 del anexo I. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 37, apartado 2. Cuando** […] elabore […] **dichos actos de ejecución**, la Comisión […] **se guiará**, en la mayor medida posible, por las normas internacionales y europeas, así como por las especificaciones técnicas pertinentes **e intercambiará recomendaciones con el Grupo de Cooperación y la ENISA sobre el proyecto de acto de ejecución de conformidad con el artículo 12, apartado 4, letra d).**

6. […]

Artículo 19

Evaluaciones coordinadas de la UE de los riesgos de las cadenas de suministro críticas

1. El Grupo de Cooperación, en colaboración con la Comisión y la ENISA, podrán llevar a cabo evaluaciones coordinadas de los riesgos de seguridad de cadenas de suministro de servicios, sistemas o productos de TIC críticos específicos, teniendo en cuenta factores de riesgo técnicos y, cuando proceda, de otra índole.

2. La Comisión, tras consultar al Grupo de Cooperación y a la ENISA, delimitará los servicios, sistemas o productos de TIC críticos específicos que podrán ser objeto de la evaluación coordinada de riesgos a que se refiere el apartado 1.

Artículo 20

Obligaciones de notificación

1. Los Estados miembros velarán por que las entidades esenciales e importantes notifiquen, sin demora indebida, a las autoridades competentes o al CSIRT de conformidad con los apartados 3 y 4 cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. Cuando proceda, dichas entidades notificarán, sin demora indebida, a los destinatarios de sus servicios los incidentes susceptibles de afectar negativamente a la prestación de dicho servicio. Los Estados miembros garantizarán que dichas entidades notifiquen, entre otros detalles, cualquier información que permita a las autoridades competentes o al CSIRT determinar las repercusiones transfronterizas del incidente. **El acto de la notificación en sí mismo no implicará una mayor responsabilidad para la entidad notificante.**

2. […]

   Cuando proceda, […] **las entidades esenciales e importantes** notificarán, sin demora indebida, a los destinatarios de sus servicios que puedan verse afectados por una ciberamenaza significativa de las medidas o soluciones que dichos destinatarios pueden aplicar en respuesta a la amenaza. Cuando proceda, las entidades notificarán a los destinatarios la propia amenaza. El **acto de la** notificación **en sí** no implicará una mayor responsabilidad para la entidad notificante.

3. Un incidente se considerará significativo si:

a) el incidente ha causado o puede causar perturbaciones operativas **del servicio** o perjuicios económicos […] **graves** para la entidad afectada;

b) el incidente ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o morales considerables.

4. Los Estados miembros velarán por que, a los efectos de la notificación con arreglo al apartado 1, las entidades afectadas presenten a las autoridades competentes o al CSIRT:

a) sin demora indebida y en cualquier caso en el plazo de veinticuatro horas desde que se haya tenido constancia del incidente, una notificación inicial **a modo de alerta temprana** en la que se indicará, cuando proceda, si cabe suponer que el incidente responde a una acción ilícita o malintencionada;

b) a instancias de una autoridad competente o un CSIRT, un informe intermedio con las actualizaciones pertinentes sobre la situación;

c) un informe **final**, a más tardar un mes después de presentar […] la **notificación inicial** contemplada en la letra a), en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente desencadenó el incidente;

iii) las medidas de mitigación aplicadas y en curso.

Los Estados miembros dispondrán que, en casos debidamente justificados y de acuerdo con las autoridades competentes o el CSIRT, la entidad afectada pueda incumplir los plazos establecidos en las letras a) y c). **En particular, un incumplimiento del plazo mencionado en la letra c) puede estar justificado cuando el incidente siga en curso.**

5. Las autoridades nacionales competentes o el CSIRT ofrecerá, […] **sin demora indebida** tras la recepción de la notificación inicial a que se refiere el apartado 4, letra a), una respuesta a la entidad notificante, en particular sus comentarios iniciales sobre el incidente y, a instancias de la entidad, una orientación sobre la aplicación de posibles medidas de mitigación. Cuando el CSIRT no haya recibido la notificación a que se refiere el apartado 1, la orientación será proporcionada por la autoridad competente en colaboración con el CSIRT. El CSIRT prestará apoyo técnico adicional cuando así lo solicite la entidad afectada. Cuando se sospeche que el incidente es de naturaleza delictiva, las autoridades nacionales competentes o el CSIRT también proporcionarán orientación a efectos de denunciar el incidente ante las autoridades policiales.

6. Cuando proceda, y en particular si el incidente mencionado en el apartado 1 afecta a dos o más Estados miembros, la autoridad competente, el CSIRT o el **punto de contacto único** al que se haya notificado el incidente informará del mismo a los demás Estados miembros afectados y a la ENISA. **Dicha información incluirá al menos los elementos mencionados en al apartado 4 del presente artículo.** Al hacerlo, las autoridades competentes, los 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 de la entidad, así como la confidencialidad de la información facilitada.

7. Cuando el conocimiento del público sea necesario para evitar un incidente o hacer frente a un incidente en curso, o cuando la divulgación del incidente redunde en el interés público, la autoridad competente o el CSIRT y, en su caso, las autoridades o CSIRT de otros Estados miembros afectados, podrán informar al público, después de consultarlo con la entidad afectada, del incidente o exigir a la entidad que lo haga.

8. A instancias de la autoridad competente o del CSIRT, el punto de contacto único remitirá las notificaciones recibidas de conformidad con el apartado […] 1 […] a los puntos de contacto únicos de otros Estados miembros afectados.

9. El punto de contacto único presentará […] **semestralmente** a la ENISA un informe de síntesis que incluya datos anonimizados y agregados sobre los incidentes, los cuasiincidentes y las ciberamenazas significativos notificados con arreglo al apartado 1 […] y al artículo 27. A fin de facilitar el suministro de información comparable, la ENISA podrá publicar orientaciones técnicas sobre los parámetros de la información que debe figurar en el informe de síntesis. **La ENISA informará semestralmente al Grupo de Cooperación y a la red de CSIRT sobre las conclusiones que haya extraído a partir de las notificaciones recibidas.**

10. Las autoridades competentes facilitarán a las autoridades competentes designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] información sobre los incidentes y las ciberamenazas notificados de conformidad con los apartados 1 y 2 por entidades esenciales identificadas como entidades críticas, **[**o como entidades equivalentes a entidades críticas,**]** conforme a lo dispuesto en dicha Directiva.

11. La Comisión podrá adoptar actos de ejecución para especificar en mayor detalle el tipo de información, el formato y el procedimiento de las notificaciones presentadas de conformidad con los apartados 1 y 2. Asimismo, la Comisión podrá adoptar actos de ejecución para precisar los casos en que un incidente se considerará significativo, tal como se contempla en el apartado 3. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 37, apartado 2.

Artículo 21

Utilización de esquemas europeos de certificación de la ciberseguridad

1. A efectos de demostrar la conformidad con determinados requisitos del artículo 18, **los Estados miembros podrán exigir a las entidades que utilicen determinados productos, servicios y procesos de TIC certificados** en virtud de un esquema europeo de certificación de la ciberseguridad específico adoptado con arreglo al artículo 49 del Reglamento (UE) 2019/881. Los productos, servicios y procesos de **TIC** objeto de la certificación podrán ser desarrollados por una entidad esencial o importante o adquiridos a terceros.

2. La Comisión […] podrá […] adoptar actos **de ejecución** que especifiquen qué categorías de entidades esenciales **o importantes** estarán obligadas **a utilizar determinados productos, servicios y procesos de TIC certificados o** a obtener una certificación y con arreglo a […] qué esquemas europeos de certificación de la ciberseguridad **adoptados de conformidad con el artículo 49 del Reglamento (UE) 2019/881**.[…] **Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 37, apartado 2. Al elaborar dichos actos de ejecución, la Comisión, con arreglo al artículo 56 del Reglamento (UE) 2019/881:**

   i) tendrá en cuenta el impacto de las medidas en los fabricantes o proveedores de productos, servicios y procesos de TIC y en los usuarios en lo que respecta al coste de dichas medidas y a los beneficios sociales o económicos que se deriven del refuerzo anticipado del nivel de seguridad para los productos, servicios y procesos de TIC en cuestión, así como la disponibilidad de otros productos, servicios y procesos de TIC en el mercado;

   ii) llevará a cabo un procedimiento de consulta abierto, transparente e inclusivo con todas las partes interesadas pertinentes y los Estados miembros;

iii) Tendrá en cuenta los plazos de aplicación, las medidas y los períodos transitorios, en particular en lo que se refiere al posible impacto de las medidas en los fabricantes o proveedores de productos, servicios o procesos de TIC, o en sus usuarios, especialmente las pymes;

iv) tendrá en cuenta la existencia y la aplicación de la legislación pertinente de los Estados miembros.

3. La Comisión podrá solicitar a la ENISA que elabore una propuesta de esquema **o que revise un esquema europeo de certificación de la ciberseguridad existente** de conformidad con el artículo 48, apartado 2, del Reglamento (UE) 2019/881 cuando no haya disponible ningún esquema europeo de certificación de la ciberseguridad apropiado a los efectos del apartado 2 **del presente artículo**.

Artículo 22

Normalización

1. A fin de promover una aplicación convergente de lo dispuesto en el artículo 18, 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 escala europea o internacionalmente que sean pertinentes en materia de seguridad de las redes y los 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 23

Bases de datos de nombres de dominio y datos de registro

1. A efectos de contribuir a la seguridad, estabilidad y resiliencia del DNS, los Estados miembros velarán por que los registros **de nombres** de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel recopilen y mantengan datos precisos y completos sobre el registro de nombres de dominio en una base de datos con la diligencia debida, **de conformidad con** […] la legislación de la Unión en materia de protección de datos por lo que respecta a los datos de carácter personal.

2. Los Estados miembros garantizarán que las bases de datos sobre el registro de nombres de dominio a que se refiere el apartado 1 contengan información pertinente para identificar y localizar a los titulares de los nombres de dominio y los puntos de contacto que administran los nombres de dominio en los dominios de primer nivel**, al menos los datos siguientes:**

   a) nombre de dominio,

   b) fecha de registro,

   c) datos sobre el titular del nombre de dominio, en particular:

      i) para las personas físicas: nombre, apellidos y dirección de correo electrónico;

      ii) para las personas jurídicas: nombre y dirección de correo electrónico.

3. Los Estados miembros se asegurarán de que los registros **de nombres** de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel cuenten con políticas y procedimientos para garantizar que las bases de datos incluyan información precisa y completa. Los Estados miembros velarán por que tales políticas y procedimientos se pongan a disposición del público.

4. Los Estados miembros garantizarán que los registros **de nombres** de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel publiquen, sin demora indebida después del registro de un nombre de dominio, los datos de registro de dominio que no sean de carácter personal.

5. Los Estados miembros se asegurarán de que los registros **de nombres** de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel concedan acceso a datos específicos sobre el registro de nombres de dominio, previa solicitud lícita y debidamente justificada, a los solicitantes de acceso legítimos, de conformidad con la legislación de la Unión en materia de protección de datos. Los Estados miembros velarán por que los registros **de nombres** de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio de primer nivel respondan sin demora indebida**, y en cualquier en un plazo de 72 horas,** a todas las solicitudes de acceso. Los Estados miembros garantizarán que las políticas y los procedimientos de divulgación de dichos datos se pongan a disposición del público.

Sección II

Jurisdicción y registro

Artículo 24

Jurisdicción y territorialidad

1 *bis* **Se considerará que las entidades incluidas en la presente Directiva están sometidas a la jurisdicción del Estado miembro en el que prestan sus servicios. Se considerará que las entidades que figuran en el anexo I, puntos 1 a 7 y 10**, **los prestadores de servicios de confianza y los proveedores de puntos de intercambio de internet mencionados en el anexo I, punto 8, y en el anexo II, puntos 1 a 5, están sometidas a la jurisdicción del Estado miembro en cuyo territorio estén establecidas.**

1. Los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel […] **y las entidades que presten servicios de registro de nombres de dominio de primer nivel**, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, […] los proveedores de redes de distribución de contenidos**, los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados** a que se refiere el anexo I, punto 8 **y punto 8 *bis***, así como los proveedores de servicios digitales a que se refiere el anexo II, punto 6, se considerarán sometidos a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal en la Unión.

2. A los efectos de la presente Directiva, se considerará que el establecimiento principal en la Unión de las entidades a que se refiere el apartado 1 se encuentra en el Estado miembro en el que se adopten **de forma predominante** las decisiones relativas a las medidas para la gestión de riesgos de ciberseguridad. En caso de que **no se pueda determinar el lugar en el que dichas decisiones se adoptan de forma predominante o** si dichas decisiones no se adoptan en un establecimiento dentro de la Unión, se considerará que el establecimiento principal se encuentra en el Estado miembro en el que las entidades tienen el establecimiento con mayor número de trabajadores en la Unión. **Cuando los servicios los preste un grupo empresarial, el establecimiento principal deberá considerarse el establecimiento principal del grupo empresarial.**

3. Si una entidad contemplada en el apartado 1 no está establecida en la Unión, pero ofrece servicios dentro de esta, designará un representante en ella. El representante se establecerá en uno de aquellos Estados miembros en los que se ofrecen los servicios. Dicha entidad se considerará sometida a la jurisdicción del Estado miembro en el que se encuentre establecido su representante. En ausencia de un representante designado dentro de la Unión con arreglo al presente artículo, cualquier Estado miembro en el que la entidad preste servicios podrá emprender acciones legales contra la entidad por incumplimiento de las obligaciones recogidas en la presente Directiva.

4. La designación de un representante por una entidad contemplada en el apartado 1 se entenderá sin perjuicio de las acciones legales que pudieran emprenderse contra la propia entidad.

4 *bis*. Los Estados miembros que hayan recibido una solicitud de asistencia mutua en relación con las entidades a que se refiere el apartado 1 podrán, dentro de los límites de la solicitud, adoptar las medidas de supervisión y ejecución adecuadas en relación con la entidad en cuestión que presta servicios o que tiene la red y el sistema de información en su territorio.

Artículo 25

Registro para determinadas entidades de infraestructuras digitales y proveedores de servicios digitales

1. […] **Los Estados miembros velarán por que** […] las entidades **mencionadas en el artículo 24, apartado 1, que tengan su establecimiento principal en su territorio o cuyo representante designado en la Unión esté establecido en su territorio, si no están establecidas en la Unión, tengan la obligación de** […] presentar la siguiente información **a las autoridades competentes** […] a más tardar [doce meses después de la entrada en vigor de la Directiva como máximo]:

a) el nombre de la entidad;

a *bis*) el tipo de entidad con arreglo a los anexos I y II de la presente Directiva;

b) la dirección de su establecimiento principal y del resto de sus establecimientos legales en la Unión o, de no estar establecida en la Unión, de su representante designado en virtud del artículo 24, apartado 3;

c) los datos de contacto actualizados, en particular las direcciones de correo electrónico y los números de teléfono de las entidades **o de sus representantes;**

d) los Estados miembros en los que la entidad presta el servicio.

Cuando corresponda, la información se presentará mediante el mecanismo nacional […] de autonotificación mencionado en el artículo 2 *bis*.

2. **Los Estados miembros velarán por que** […] las entidades a que se refiere el apartado 1 […] **notifiquen también** cualquier cambio en la información remitida con arreglo al apartado 1 sin demora, y en cualquier caso, en el plazo de tres meses desde la fecha en que se produjo el cambio.

3. […] **Los puntos de contacto únicos de los Estados miembros** remitirán **la información mencionada en los apartados 1 y 2** […] a […] **la ENISA**. […]

3 *bis*. Sobre la base de la información recibida de conformidad con el apartado 3 del presente artículo, la ENISA creará y mantendrá un registro de las entidades a que se refiere el apartado 1. A petición de los Estados miembros, la ENISA permitirá el acceso de las autoridades competentes pertinentes al registro, garantizando al mismo tiempo las garantías necesarias para proteger la confidencialidad de la información cuando proceda.

4. […]

CAPÍTULO V

Intercambio de información

Artículo 26

Mecanismos de intercambio de información sobre ciberseguridad

1. […] Los Estados miembros velarán por que las entidades esenciales e importantes puedan intercambiar **de forma voluntaria** información sobre ciberseguridad pertinente, en particular la referente a ciberamenazas, **cuasiincidentes**, vulnerabilidades, indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, siempre que dicho intercambio de información:

   a) se haga con el objetivo de prevenir, detectar, responder o mitigar incidentes;

b) refuerce el nivel de ciberseguridad, en particular al concienciar sobre las ciberamenazas, limitar o impedir la capacidad de tales amenazas para propagarse, o respaldar una batería de capacidades de defensa, corrección y divulgación de las vulnerabilidades, técnicas de detección de amenazas, estrategias de mitigación o etapas de respuesta y recuperación.

2. Los Estados miembros garantizarán que el intercambio de información se desarrolle dentro de comunidades […] de entidades esenciales e importantes. Dicho intercambio se pondrá en práctica a través de mecanismos de intercambio de información que respeten la posible naturaleza delicada de la información compartida […].

3. Los Estados miembros […] **podrán** establecer normas que precisen el procedimiento, los elementos operativos (incluido el uso de plataformas de TIC específicas), el contenido y las condiciones de los mecanismos de intercambio de información a que se refiere el apartado 2. Asimismo, dichas normas […] **podrán** establecer los detalles de la participación de las autoridades públicas en los mecanismos mencionados, así como los elementos operativos, incluido el uso de plataformas de TIC específicas. Los Estados miembros prestarán apoyo a la aplicación de dichos mecanismos de conformidad con las correspondientes políticas a que se refiere el artículo 5, apartado 2, letra g).

4. Las entidades esenciales e importantes notificarán a las autoridades competentes su participación en los mecanismos de intercambio de información a que se refiere el apartado 2 cuando se incorporen a dichos mecanismos o, cuando proceda, su retirada de dichos mecanismos cuando la retirada surta efecto.

5. […] La ENISA prestará su apoyo al establecimiento de mecanismos de intercambio de información sobre ciberseguridad a que se refiere el apartado 2 mediante el suministro de buenas prácticas y orientación.

Artículo 27

Notificación voluntaria de información pertinente

1. Sin perjuicio de lo dispuesto en el artículo 20, los Estados miembros velarán por que las entidades esenciales e importantes puedan notificar, de forma voluntaria, a las autoridades competentes o a los CSIRT cualquier incidente, ciberamenaza o cuasiincidente pertinente.

2. Los Estados miembros velarán por que, sin perjuicio de lo dispuesto en el artículo 3, las entidades excluidas del ámbito de aplicación de la presente Directiva puedan presentar voluntariamente notificaciones de ciberamenazas, cuasiincidentes e incidentes significativos. Cuando tramiten las notificaciones, los Estados miembros actuarán de conformidad con el procedimiento establecido en el artículo 20. Los Estados miembros podrán dar prioridad a la tramitación de notificaciones obligatorias sobre las notificaciones voluntarias. **Sin perjuicio de la investigación, detección y enjuiciamiento de infracciones penales,** […] **la** notificación voluntaria no dará lugar a la imposición a la entidad notificante de obligaciones adicionales a las que no estaría sujeta de no haber presentado dicha notificación.

3. Las notificaciones voluntarias se tramitarán únicamente cuando dicha tramitación no suponga una carga desproporcionada o indebida para el Estado miembro de que se trate.

CAPITULO VI

Supervisión y ejecución

Artículo 28

Aspectos generales relativos a la supervisión y la ejecución

1. Los Estados miembros velarán por que las autoridades competentes supervisen efectivamente y adopten las medidas necesarias para garantizar el cumplimiento de la presente Directiva, en particular de las obligaciones establecidas en los artículos 18**,** […] 20 y 2**3**. **Los Estados miembros podrán autorizar a las autoridades competentes a priorizar la supervisión, que se fundamentará en un planteamiento basado en el riesgo.**

2. Las autoridades competentes cooperarán estrechamente con las autoridades responsables de la protección de datos, **las autoridades competentes designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas], los organismos de supervisión designados en virtud del Reglamento (UE) n.º 910/2014 y otras autoridades competentes designadas en virtud de actos jurídicos de la Unión de carácter sectorial** a la hora de hacer frente a incidentes de ciberseguridad. […]

3. Sin perjuicio de los marcos legislativos e institucionales nacionales, los Estados miembros garantizarán que, en el contexto de la supervisión del cumplimiento de la presente Directiva por las entidades de la Administración pública y de la ejecución de posibles sanciones en caso de incumplimiento, las autoridades competentes dispongan de las competencias adecuadas para llevar a cabo dichas tareas con independencia operativa con respecto a las entidades supervisadas. Los Estados miembros podrán decidir imponer medidas de supervisión y ejecución adecuadas, proporcionadas y eficaces en relación con dichas entidades, de conformidad con los marcos y el ordenamiento jurídico nacionales.

Artículo 29

Supervisión y ejecución en el caso de entidades esenciales

1. Los Estados miembros garantizarán que las medidas de supervisión o ejecución impuestas a las entidades esenciales en relación con las obligaciones contempladas en la presente Directiva sean efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual.

2. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus funciones de supervisión en relación con entidades esenciales, **apliquen un planteamiento basado en el riesgo y** dispongan de competencias para someter a dichas entidades **como mínimo** a:

   a) inspecciones *in situ* y supervisión a distancia, incluidos controles aleatorios;

   b) auditorías **de seguridad** periódicas;

   c) auditorías de seguridad específicas basadas en evaluaciones de riesgos o en información disponible sobre los riesgos;

   d) análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes, **cuando sea necesario por motivos técnicos, con la cooperación de la entidad afectada**;

   e) solicitudes de información necesaria para evaluar las medidas de ciberseguridad adoptadas por la entidad, en particular las políticas de ciberseguridad documentadas […];

   f) solicitudes de acceso a datos, documentos o cualquier información necesaria para el desempeño de sus funciones de supervisión;

   g) solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.

2 *bis*. Cuando ejecuten sus tareas de supervisión, establecidas en el apartado 2 del presente artículo, las autoridades competentes podrán establecer metodologías de supervisión que permitan priorizar dichas tareas aplicando un planteamiento basado en el riesgo.

3. En el ejercicio de sus competencias con arreglo al apartado 2, letras e), f) y g), las autoridades competentes indicarán la finalidad de la solicitud y especificarán la información requerida.

4. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus facultades de ejecución en relación con entidades esenciales, dispongan de competencias **como mínimo** para:

a) apercibir a las entidades por el incumplimiento de las obligaciones establecidas en la presente Directiva;

b) emitir instrucciones vinculantes o una orden de requerimiento para que dichas entidades subsanen las deficiencias detectadas o las infracciones de las obligaciones establecidas en la presente Directiva;

c) exigir a dichas entidades que pongan fin a las conductas que incumplan las obligaciones establecidas en la presente Directiva y que se abstengan de repetirlas;

d) exigir a dichas entidades que adecúen sus medidas de gestión de riesgos u obligaciones de notificación a las obligaciones establecidas en los artículos 18 y 20 de una manera específica y en un plazo concreto;

e) ordenar a dichas entidades que informen a las personas físicas o jurídicas a las que prestan servicios o actividades que puedan verse afectadas por una ciberamenaza significativa de **la naturaleza de la amenaza, así como de** cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza;

f) ordenar a dichas entidades que apliquen las recomendaciones formuladas a raíz de una auditoría de seguridad en un plazo razonable;

g) […]

h) ordenar a dichas entidades que hagan públicos aspectos del incumplimiento de las obligaciones establecidas en la presente Directiva de una manera específica, **cuando dicha divulgación no conlleve una exposición perjudicial de la entidad de que se trate**;

i) […]

j) imponer o solicitar la imposición por parte de los organismos o los órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 31 a título adicional o sustitutivo de las medidas referidas en las letras a) a i) del presente apartado, en función de las circunstancias de cada caso particular.

5. Cuando las medidas de ejecución adoptadas con arreglo al apartado 4, letras a) a d) y f), resulten ineficaces, los Estados miembros garantizarán que las autoridades competentes estén facultadas para fijar un plazo en el que se requerirá a la entidad esencial que adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de dichas autoridades. Si las medidas requeridas no se adoptan dentro del plazo establecido, los Estados miembros velarán por que las autoridades competentes estén facultadas para:

a) suspender o solicitar a un organismo de certificación o autorización **o a un órgano jurisdiccional de acuerdo con la legislación nacional** que suspenda una certificación o autorización referente a una parte o la totalidad de los servicios o actividades prestados por una entidad esencial;

b) imponer o solicitar la imposición por parte de los organismos o los órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una prohibición temporal sobre cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial, y de cualquier otra persona física responsable del incumplimiento, de ejercer funciones de dirección en dicha entidad.

Las sanciones referidas se aplicarán únicamente hasta que la entidad adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente a instancias de la cual se aplicaron las sanciones.

Las sanciones previstas en el presente apartado no son aplicables a las entidades de la Administración pública sujetas a la presente Directiva.

6. Los Estados miembros garantizarán que cualquier persona física responsable de una entidad esencial o que actúe como representante de ella con facultades para representarla, la autoridad para tomar decisiones en su nombre o la autoridad para ejercer control sobre ella tenga competencias para velar por que cumpla las obligaciones establecidas en la presente Directiva. Los Estados miembros velarán por que dichas personas físicas puedan considerarse responsables por el incumplimiento de su deber de garantizar el cumplimiento de las obligaciones establecidas en la presente Directiva. **Por lo que respecta a las entidades de la Administración pública, la presente disposición se entenderá sin perjuicio de la legislación de los Estados miembros relativa a la responsabilidad de los funcionarios y de los cargos electos y designados.**

7. Cuando se adopte una medida de ejecución o se aplique una sanción con arreglo a los apartados 4 y 5, las autoridades competentes observarán el derecho de defensa y tendrán en cuenta las circunstancias de cada caso particular, como mínimo los siguientes aspectos:

   a) la gravedad del incumplimiento y la importancia de las disposiciones infringidas. Entre las infracciones que deben considerarse graves cabe destacar los incumplimientos reiterados, la ausencia de notificación o subsanación de los incidentes con un efecto perturbador significativo, la ausencia de subsanación de deficiencias tras recibir instrucciones vinculantes de las autoridades competentes, la obstrucción de las actividades de fiscalización o control ordenadas por la autoridad competente tras la constatación de una infracción, el suministro de información falsa o manifiestamente imprecisa en relación con los requisitos de gestión del riesgo o las obligaciones de notificación previstos en los artículos 18 y 20.

b) la duración del incumplimiento, en particular si ha habido incumplimientos reiterados;

c) los perjuicios o las pérdidas reales originados, o los perjuicios o las pérdidas que podrían haberse originado, en la medida en que puedan determinarse. A la hora de evaluar este aspecto, se tendrán en cuenta, entre otros factores, las pérdidas financieras o económicas reales o potenciales, los efectos para otros servicios y el número de usuarios afectados o potencialmente afectados;

d) la intencionalidad o negligencia en la infracción;

e) las medidas adoptadas por la entidad para prevenir o reducir los perjuicios o las pérdidas;

f) la adhesión a códigos de conducta o a mecanismos de certificación aprobados;

g) el grado de cooperación de las personas físicas o jurídicas responsables con las autoridades competentes.

8. Las autoridades competentes argumentarán detalladamente sus decisiones de ejecución. Antes de tomar dichas decisiones, las autoridades competentes notificarán a las entidades afectadas sus constataciones preliminares y concederán a dichas entidades un plazo razonable para formular observaciones**, salvo en caso de peligro inminente**.

9. Los Estados miembros velarán por que sus autoridades competentes **con arreglo a la presente Directiva** informen a las autoridades competentes pertinentes **dentro del mismo** […] Estado miembro […] designadas en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] cuando ejerzan sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento por parte de una entidad esencial identificada como crítica, **[**o como una entidad equivalente a una entidad crítica**]**, con arreglo a dicha Directiva, de las obligaciones conforme a la presente Directiva. **Cuando proceda,** […] las autoridades competentes en virtud de la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas] […] **podrán solicitar a** las autoridades competentes **en virtud** de la presente Directiva […] ejercer sus **facultades** de supervisión y ejecución **en relación con** una entidad esencial que entre en el ámbito de aplicación de la presente Directiva y que haya sido también identificada como crítica **[**o equivalente**] con arreglo a la Directiva (UE) XXXX/XXXX [Directiva sobre la resiliencia de las entidades críticas]**.

10. Los Estados miembros velarán por que sus autoridades competentes con arreglo a la presente Directiva informen al Foro de Supervisión establecido de conformidad con el artículo 29, apartado 1, del Reglamento (UE) XXXX/XXXX [DORA] cuando ejerzan sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento por parte de una entidad esencial identificada como proveedor tercero esencial de servicios de TIC de conformidad con el artículo 28 del Reglamento (UE) XXXX/XXXX [DORA] de las obligaciones conforme a la presente Directiva.

10 *bis*. Los Estados miembros velarán por que sus autoridades competentes con arreglo a la presente Directiva informen a las autoridades competentes pertinentes designadas en virtud del Reglamento (UE) n.º 910/2014 cuando ejerzan sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento por parte de una entidad identificada como prestador de servicios de confianza con arreglo a dicho Reglamento de las obligaciones conforme a la presente Directiva.

Artículo 30

Supervisión y ejecución en el caso de entidades importantes

1. Cuando dispongan de pruebas o indicios **o información** de que una entidad importante **presuntamente** no cumple las obligaciones establecidas en la presente Directiva, y en particular en los artículos 18 y 20, los Estados miembros garantizarán que las autoridades competentes actúen, cuando proceda, a través de medidas de supervisión *a posteriori*.

2. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus tareas de supervisión en relación con entidades importantes, **apliquen un planteamiento basado en el riesgo y** dispongan de competencias para someter a dichas entidades **como mínimo** a:

   a) inspecciones *in situ* y supervisión *a posteriori* a distancia;

   b) auditorías de seguridad específicas basadas en evaluaciones de riesgos o en información disponible sobre los riesgos;

   c) análisis de seguridad basados en criterios de evaluación del riesgo objetivos, **no discriminatorios,** justos y transparentes**, cuando sea necesario por motivos técnicos, con la cooperación de la entidad afectada**;

   d) solicitudes de toda información necesaria para evaluar a posteriori las medidas de ciberseguridad […];

   e) solicitudes de acceso a datos, documentos o cualquier información necesaria para el desempeño de las funciones de supervisión;

   e *bis*) solicitudes de pruebas de la aplicación de las políticas de ciberseguridad, como por ejemplo los resultados de las auditorías de seguridad realizadas por un auditor cualificado y las correspondientes pruebas subyacentes.

2 *bis*. Cuando lleven a cabo sus tareas de supervisión, establecidas en el apartado 2 del presente artículo, las autoridades competentes podrán establecer metodologías de supervisión que permitan priorizar dichas tareas aplicando un planteamiento basado en el riesgo.

3. En el ejercicio de sus competencias con arreglo al apartado 2, letras d)**, e) y e *bis*)**, las autoridades competentes indicarán la finalidad de la solicitud y especificarán la información requerida.

4. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus facultades de ejecución en relación con entidades importantes, dispongan de competencias **como mínimo** para:

   a) apercibir a las entidades por el incumplimiento de las obligaciones establecidas en la presente Directiva;

   b) emitir instrucciones vinculantes o una orden de requerimiento para que dichas entidades subsanen las deficiencias detectadas o la infracción de las obligaciones establecidas en la presente Directiva;

   c) exigir a dichas entidades que pongan fin a las conductas que incumplan las obligaciones establecidas en la presente Directiva y que se abstengan de repetirlas;

   d) exigir a dichas entidades que adecúen sus medidas de gestión de riesgos u obligaciones de notificación a las obligaciones establecidas en los artículos 18 y 20 de una manera específica y en un plazo concreto;

   e) ordenar a dichas entidades que informen a las personas físicas o jurídicas a las que prestan servicios o actividades que puedan verse afectadas por una ciberamenaza significativa **de la naturaleza de la amenaza, así como de** cualquier posible medida correctora o de protección que dichas personas puedan adoptar en respuesta a la amenaza;

   f) ordenar a dichas entidades que apliquen las recomendaciones formuladas a raíz de una auditoría de seguridad en un plazo razonable;

g) ordenar a dichas entidades que hagan públicos aspectos del incumplimiento de sus obligaciones establecidas en la presente Directiva de una manera específica, **cuando dicha divulgación no conlleve una exposición perjudicial de la entidad de que se trate**;

h) […]

i) imponer o solicitar la imposición por parte de los órganos o tribunales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 31 a título adicional o sustitutivo de las medidas referidas en las letras a) a h) del presente apartado, en función de las circunstancias de cada caso particular.

5. El artículo 29, apartados 6, 7 y 8, se aplicará asimismo a las medidas de supervisión y ejecución previstas en el presente artículo en el caso de […] entidades importantes […].

Artículo 31

Condiciones generales para la imposición de multas administrativas a entidades esenciales e importantes

1. Los Estados miembros velarán por que las multas administrativas impuestas a entidades esenciales e importantes al amparo del presente artículo en relación con el incumplimiento de las obligaciones establecidas en la presente Directiva sean, en cada caso particular, efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 29, apartado 4, letras a) a i), el artículo 29, apartado 5, y el artículo 30, apartado 4, letras a) a h).

3. A la hora de decidir la imposición de una multa administrativa y su cuantía en cada caso particular se tendrán debidamente en cuenta, como mínimo, los elementos contemplados en el artículo 29, apartado 7.

4. Los Estados miembros garantizarán que el incumplimiento **por las entidades esenciales** de las obligaciones establecidas en los artículos 18 o 20 se sancione, de acuerdo con los apartados 2 y 3 del presente artículo, con multas administrativas cuya cuantía máxima debe ser al menos **4**[…] 000 000 EUR o**, en el caso de una persona jurídica,** […] el 2 % del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad esencial durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

4 *bis*. Los Estados miembros garantizarán que el incumplimiento por las entidades importantes de las obligaciones establecidas en los artículos 18 o 20 se sancione, de acuerdo con los apartados 2 y 3 del presente artículo, con multas administrativas cuya cuantía máxima debe ser al menos 2 000 000 EUR o, en el caso de una persona jurídica, el 1 % del volumen de negocios anual total a nivel mundial de la empresa a la que pertenece la entidad importante durante el ejercicio financiero anterior, optándose por la de mayor cuantía.

5. Los Estados miembros pueden prever la facultad de imponer multas coercitivas para obligar a una entidad esencial o importante a poner fin a una infracción de conformidad con una decisión previa de la autoridad competente.

6. Sin perjuicio de las facultades de las autoridades competentes conferidas en virtud de los artículos 29 y 30, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a las entidades de la Administración pública a que se refiere el artículo 4, punto 23, sujetas a las obligaciones previstas en la presente Directiva.

6 *bis*. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, los Estados miembros velarán por que el presente artículo pueda aplicarse de tal modo que la incoación de la multa corresponda a la autoridad competente y su imposición a los órganos jurisdiccionales nacionales competentes, garantizando al mismo tiempo que estas vías de recurso sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades competentes. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el […] y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 32

Infracciones que conllevan una violación de la seguridad de los datos personales

1. Cuando**, en el transcurso de las actividades de supervisión o ejecución,** las autoridades competentes […] **adquieran constancia** de que el incumplimiento de las obligaciones establecidas en los artículos 18 y 20 **de la presente Directiva** […] por una entidad esencial o importante **podría** conllevar una violación de la seguridad de los datos personales en el sentido del artículo 4, punto 12, del Reglamento (UE) 2016/679 que deba notificarse en virtud del artículo 33 de dicho Reglamento, informarán**, sin dilación indebida,** a las autoridades de control competentes en virtud de los artículos 55 y 56 de dicho Reglamento […].

2. Cuando las autoridades de control competentes de conformidad con los artículos 55 y 56 del Reglamento (UE) 2016/679 decidan ejercer sus facultades con arreglo al artículo 58, apartado 2, letra i), de dicho Reglamento e imponer una multa administrativa, las autoridades competentes **a que se refiere el artículo 8 de la presente Directiva** no impondrán una multa administrativa por […] **una** infracción **por el mismo hecho de lo dispuesto en el** […] artículo 31 de la presente Directiva. No obstante lo dispuesto, las autoridades competentes podrán aplicar las medidas de ejecución o ejercer las facultades sancionadoras previstas en el artículo 29, apartado 4, letras a) a i), el artículo 29, apartado 5, y el artículo 30, apartado 4, letras a) a h), de la presente Directiva.

3. Cuando la autoridad de control competente en virtud del Reglamento (UE) 2016/679 esté establecida en un Estado miembro distinto al de la autoridad competente, la autoridad competente podrá informar a la autoridad de control establecida en el mismo Estado miembro.

Artículo 33

Sanciones

1. Los Estados miembros establecerán el régimen de sanciones aplicables a cualquier infracción de las disposiciones nacionales adoptadas al amparo de la presente Directiva y adoptarán todas las medidas necesarias para garantizar su ejecución. Tales sanciones serán efectivas, proporcionadas y disuasorias.

2. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, a más tardar [dos] años después de la entrada en vigor de la presente Directiva, y le notificarán sin demora indebida cualquier modificación posterior.

Artículo 34

Asistencia mutua

1. Cuando una entidad esencial o importante preste servicios en más de un Estado miembro, o […] **preste servicios** en un**o o varios** Estado**s** miembro**s**, pero sus redes y sistemas de información estén situados en otro u otros Estados miembros, la**s** autoridad**es** competente**s** de **los** Estado**s** miembro**s de que se trate** […] cooperarán entre sí y se asistirán mutuamente cuando sea necesario. Dicha cooperación implicará, como mínimo, lo siguiente:

a) que las autoridades competentes que apliquen medidas de supervisión o ejecución en un Estado miembro informen y consulten a través del punto de contacto único a las autoridades competentes de los otros Estados miembros afectados sobre las medidas de supervisión y ejecución adoptadas […];

b) que una autoridad competente pueda solicitar a otra autoridad competente que adopte las medidas de supervisión o ejecución […];

c) que una autoridad competente, al recibir una solicitud justificada de otra autoridad competente, preste a la otra autoridad competente una asistencia **proporcionada a los recursos de los que dispone** para que las medidas de supervisión o ejecución […] puedan aplicarse de manera efectiva, eficiente y coherente. Dicha asistencia mutua podrá abarcar solicitudes de información y medidas de supervisión, incluidas las solicitudes para la realización de inspecciones *in situ*, supervisión a distancia o auditorías de seguridad específicas. La autoridad competente destinataria de una solicitud de asistencia no podrá negarse a ella a menos que, tras dialogar con las otras autoridades interesadas […], se determine que […] la autoridad carece de competencias para prestar la asistencia requerida**, que no dispone de los recursos adecuados**, que dicha asistencia no se adecúa a las tareas de supervisión de la autoridad competente desempeñadas […] **o que la solicitud se refiere a información o implica actividades que entran en conflicto con la seguridad nacional, la seguridad pública o la defensa de dicho Estado miembro**.

2. Cuando proceda y de común acuerdo, las autoridades competentes de Estados miembros diferentes podrán emprender las medidas conjuntas de supervisión […].

CAPÍTULO VII

Disposiciones transitorias y finales

Artículo 35

Revisión

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. En concreto, el informe evaluará la importancia de los sectores, los subsectores, el tamaño y el tipo de las entidades a que se refieren los anexos I y II para el funcionamiento de la economía y la sociedad por lo que respecta a la ciberseguridad. A […] efecto**s de la revisión,** […], la Comisión tendrá en cuenta los informes […] de la red de CSIRT sobre la experiencia adquirida a nivel […] operativo. El primer informe se presentará a más tardar el… [cincuenta y cuatro meses después de la fecha de entrada en vigor de la presente Directiva].

Artículo 36

[…]

[…]

[…]

Artículo 37

Procedimiento de comité

1. La Comisión estará asistida por un comité. 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, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

3. Cuando el dictamen del comité deba obtenerse mediante procedimiento escrito, se pondrá fin a dicho procedimiento sin resultado si, en el plazo para la emisión del dictamen, el presidente del comité así lo decide o si un miembro del comité así lo solicita.

Artículo 38

Transposición

1. **A más tardar el** … [[…] **veinticuatro** meses después de la fecha de entrada en vigor de la presente Directiva**], l**os Estados miembros adoptarán y publicarán […] 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 dichas disposiciones a partir del … [un día después de la fecha mencionada en el párrafo primero].

2. 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.

Artículo 39

Modificación del Reglamento (UE) n.º 910/2014

En el Reglamento (UE) n.º 910/2014, se suprime el artículo 19 […] **con efectos a partir del… [fecha del plazo de transposición de la presente Directiva]**.

Artículo 40

Modificación de la Directiva (UE) 2018/1972

En la Directiva (UE) 2018/1972, se suprimen los artículos 40 y 41 […] **con efectos a partir del… [fecha del plazo de transposición de la presente Directiva]**.

Artículo 41

Derogación

Queda derogada la Directiva (UE) 2016/1148 con efectos a partir del… [fecha del plazo de transposición de la Directiva].

Las referencias a la Directiva (UE) 2016/1148 se entenderán hechas a la presente Directiva y se leerán con arreglo a la tabla de correspondencias que figura en el anexo II[…].

Artículo 42

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 43

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente / La Presidenta	*El Presidente / La Presidenta*

ANEXO I

SECTORES, SUBSECTORES Y TIPOS DE ENTIDADES

Sector	Subsector	Tipo de entidad
1. Energía	a) Electricidad	— Las empresas eléctricas a que se refiere el artículo 2, punto 57, de la Directiva (UE) 2019/944 que realicen la función de «suministro» a que hace referencia el artículo 2, punto 12, de dicha Directiva([39]).
		— Los gestores de la red de distribución a que se refiere el artículo 2, punto 29, de la Directiva (UE) 2019/944
		— Los gestores de la red de transporte a que se refiere el artículo 2, punto 35, de la Directiva (UE) 2019/944
		— Los productores a que se refiere el artículo 2, punto 38, de la Directiva (UE) 2019/944
		— Los operadores designados para el mercado eléctrico a que se refiere el artículo 2, punto 8, del Reglamento (UE) 2019/943([40])
		— Los participantes en el mercado de la electricidad a que se refiere el artículo 2, punto 25, del Reglamento (UE) 2019/943 que presten servicios de agregación, respuesta de demanda o almacenamiento de energía, tal como se contempla en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944

[39] Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE (DO L 158 de 14.6.2019, p. 125).

[40] Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad (DO L 158 de 14.6.2019, p. 54).

	b) Sistemas urbanos de calefacción y de refrigeración	— Los sistemas urbanos de calefacción o de refrigeración a que se refiere el artículo 2, punto 19, de la Directiva (UE) 2018/2001 relativa al fomento del uso de energía procedente de fuentes renovables([41])
	c) Crudo	— Operadores de oleoductos de transporte de crudo
		— Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
		— Las entidades centrales de almacenamiento de crudo a que se refiere el artículo 2, letra f), de la Directiva 2009/119/CE([42])
	d) Gas	— Las empresas suministradoras a que se refiere el artículo 2, punto 8, de la Directiva 2009/73/CE([43])
		— Los gestores de la red de distribución a que se refiere el artículo 2, punto 6, de la Directiva 2009/73/CE
		— Los gestores de la red de transporte a que se refiere el artículo 2, punto 4, de la Directiva 2009/73/CE
		— Los gestores de almacenamientos a que se refiere el artículo 2, punto 10, de la Directiva 2009/73/CE

41 Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, relativa al fomento del uso de energía procedente de fuentes renovables (DO L 328 de 21.12.2018, p. 82).

42 Directiva 2009/119/CE del Consejo, de 14 de septiembre de 2009, por la que se obliga a los Estados miembros a mantener un nivel mínimo de reservas de petróleo crudo o productos petrolíferos (DO L 265 de 9.10.2009, p. 9).

43 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).

		— Los gestores de la red de GNL a que se refiere el artículo 2, punto 12, de la Directiva 2009/73/CE
		— Las compañías de gas natural a que se refiere el artículo 2, punto 1, de la Directiva 2009/73/CE
		— Operadores de instalaciones de refinado y tratamiento de gas natural
	e) Hidrógeno	Operadores de producción, almacenamiento y transporte de hidrógeno
2. Transporte	a) Transporte aéreo	— Las compañías aéreas a que se refiere el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008([44]) **utilizadas con fines comerciales**
		— Las entidades gestoras de aeropuertos a que se refiere el artículo 2, punto 2, de la Directiva 2009/12/CE([45]), los aeropuertos a que se refiere el artículo 2, punto 1, de dicha Directiva, en particular los aeropuertos de la red básica enumerados en el anexo II, sección 2, del Reglamento (UE) n.º 1315/2013([46]), y las entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos
		— Operadores de control de la gestión del tráfico que prestan servicios de control del tránsito aéreo a que se

[44] 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).

[45] 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).

[46] Reglamento (UE) 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).

		refiere el artículo 2, punto 1, del Reglamento (CE) n.º 549/2004([47])
	b) Transporte por ferrocarril	— Los administradores de infraestructuras a que se refiere el artículo 3, punto 2, de la Directiva 2012/34/UE([48])
		— Las empresas ferroviarias a que se refiere el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio contemplados en el artículo 3, punto 12, de dicha Directiva
	c) Transporte marítimo y fluvial	— Las empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, a que se refiere para el transporte marítimo el anexo I del Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo([49]), sin incluir los buques particulares explotados por esas empresas.
		— Los organismos gestores de los puertos a que se refiere el artículo 3, punto 1, de la Directiva 2005/65/CE([50]), incluidas sus instalaciones portuarias contempladas en el artículo 2, punto 11, del Reglamento (CE) n.º 725/2004, y las entidades que operan con las obras y equipos que se encuentran en los puertos.

47 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).

48 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).

49 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).

50 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).

		— Los operadores de servicios de tráfico de buques a que se refiere el artículo 3, letra o), de la Directiva 2002/59/CE([51])
	d) Transporte por carretera	— Las autoridades viarias a que se refiere el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión([52]) responsables del control de la gestión del tráfico**, excepto las entidades públicas para las que la gestión del tráfico o los operadores de sistemas de transporte inteligentes constituye solo una parte no esencial de su actividad general**
		— Los operadores de sistemas de transporte inteligentes a que se refiere el artículo 4, punto 1, de la Directiva 2010/40/UE([53])
3. Banca		— Las entidades de crédito a que se refiere el artículo 4, punto 1, del Reglamento (UE) n.º 575/2013 ([54])**, [excepto aquellas a que se refiere el articulo 2, apartado 5, punto 8, de la Directiva 2013/36/UE que están excluidas de conformidad con el artículo 2, apartado 4, del Reglamento XX [Reglamento sobre la resiliencia operativa digital del sector financiero]]**

[51] 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).

[52] 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).

[53] 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).

[54] 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 las 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).

4. Infraestructuras de los mercados financieros		— Los gestores de centros de negociación a que se refiere el artículo 4, punto 24, de la Directiva 2014/65/UE([55])
		— Las entidades de contrapartida central (ECC) a que se refiere el artículo 2, punto 1, del Reglamento (UE) n.º 648/2012([56])
5. Sector sanitario		— Los prestadores de asistencia sanitaria a que se refiere el artículo 3, letra g), de la Directiva 2011/24/UE([57])
		— Los laboratorios de referencia de la UE a que se refiere el artículo 15 del Reglamento XXXX/XXXX sobre las amenazas transfronterizas graves para la salud[58]
		— Las entidades que realizan actividades de investigación y desarrollo de medicamentos a que se refiere el artículo 1, punto 2, de la Directiva 2001/83/CE([59]) — Las entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2 — Las entidades que fabrican productos sanitarios que se

[55] 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).

[56] 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).

[57] 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).

[58] [Reglamento del Parlamento Europeo y del Consejo sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.º 1082/2013/UE; referencia por actualizar una vez adoptada la propuesta COM (2020)727]

[59] Directiva 2001/83/CE del Parlamento Europeo y del Consejo, de 6 de noviembre de 2001, por la que se establece un código comunitario sobre medicamentos para uso humano (DO L 311 de 28.11.2001, p. 67).

		consideran esenciales en situaciones de emergencia de salud pública («la lista de productos sanitarios esenciales durante la emergencia de salud pública») a que se refiere el artículo 20 del Reglamento XXXX[60]
6. Agua potable		Los suministradores y distribuidores de aguas destinadas al consumo humano a que se refiere el artículo 2, punto 1, letra a), de la Directiva 98/83/CE del Consejo([61]), pero sin incluir a los distribuidores para los que la distribución de aguas destinadas al consumo humano constituye solo una parte **no esencial** de su actividad general de distribución de otros bienes y productos básicos […]
7. Aguas residuales		Las empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas e industriales a que se refiere el artículo 2, puntos 1 a 3, de la Directiva 91/271/CEE del Consejo([62])**, pero sin incluir a las empresas para las que la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas e industriales constituye solo una parte no esencial de su actividad general** […]
8. Infraestructura digital		**—** Proveedores de puntos de intercambio de internet
		— Proveedores de servicios de DNS**, sin incluir a los operadores de servidores raíz**
		— Registros de nombres de dominio de primer nivel
		— Proveedores de servicios de computación en nube

60 [Reglamento del Parlamento Europeo y del Consejo relativo al papel reforzado de la Agencia Europea de Medicamentos en la preparación y gestión de crisis con respecto a los medicamentos y los productos sanitarios; referencia por actualizar una vez adoptada la propuesta COM (2020) 725]

61 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).

62 Directiva del Consejo 91/271/CEE, de 21 de mayo de 1991, sobre el tratamiento de las aguas residuales urbanas (DO L 135 de 30.5.1991, p. 40).

		— Proveedores de servicios de centro de datos
		— Proveedores de redes de distribución de contenidos
		— Los prestadores de servicios de confianza a que se refiere el artículo 3, punto 19, del Reglamento (UE) n.º 910/2014([63])
		— Los proveedores de redes públicas de comunicaciones electrónicas a que se refiere el artículo 2, punto 8, de la Directiva (UE) 2018/1972([64]) o los proveedores de servicios de comunicaciones electrónicas contemplados en el artículo 2, punto 4, de dicha Directiva cuando sus servicios estén disponibles para el público
8 *bis*. Gestión de servicios de TIC **(B2B)**		**— Proveedores de servicios gestionados** **— Proveedores de servicios de seguridad gestionados**

[63] 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).

[64] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

9. **Entes de la** Administración pública		— Entes públicos de la Administración central **según definición del Estado miembro con arreglo a las disposiciones del Derecho nacional** — […][65][…] — […]
10. Espacio		— Operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación descansa en los Estados miembros o en entidades privadas, que apoyan la prestación de servicios espaciales, excepto los proveedores de redes públicas de comunicaciones electrónicas a que se refiere el artículo 2, punto 8, de la Directiva (UE) 2018/1972

65 [...]

ANEXO II

SECTORES, SUBSECTORES Y TIPOS DE ENTIDADES

Sector	Subsector	Tipo de entidad
1. Servicios postales y de mensajería		Los proveedores de servicios postales a que se refiere el artículo 2, punto 1[…], de la Directiva 97/67/CE([66]), **incluidos** […] los proveedores de servicios de mensajería
2. Gestión de residuos		Las empresas que realizan la gestión de residuos a que se refiere el artículo 3, punto 9, de la Directiva 2008/98/CE([67]), excepto aquellas para las que la gestión de residuos no es su principal actividad económica

[66] Directiva 97/67/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio (DO L 15 de 21.1.1998, p. 14)**, modificada por la Directiva 2008/6/CE del Parlamento Europeo y del Consejo, de 20 de febrero de 2008, por la que se modifica la Directiva 97/67/CE en relación con la plena realización del mercado interior de servicios postales comunitarios (DO L 52 de 27.2.2008, p. 3)**.

[67] Directiva 2008/98/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre los residuos y por la que se derogan determinadas Directivas (DO L 312 de 22.11.2008, p. 3).

3. Fabricación, producción y distribución de sustancias y mezclas químicas		Las empresas que realizan la fabricación[…] y distribución de sustancias y […] **mezclas** a que se refiere el artículo 3, puntos […] 9 y 14, del Reglamento (CE) n.º 1907/2006([68]) **y las empresas que realizan la producción de artículos a que se refiere el artículo 3, punto 3, de dicho Reglamento a partir de sustancias o mezclas**
4. Producción, transformación y distribución de alimentos		Las empresas alimentarias a que se refiere el artículo 3, punto 2, del Reglamento (CE) n.º 178/2002([69]) **que participan en la distribución mayorista y la elaboración y la producción industrial**
5. Fabricación	a) Fabricación de productos sanitarios y productos sanitarios para diagnóstico *in vitro*	Las entidades que fabrican los productos sanitarios a que se refiere el artículo 2, punto 1, del Reglamento (UE) 2017/745([70]) y las entidades que fabrican los productos sanitarios para diagnóstico *in vitro* contemplados en el artículo 2, punto 2, del Reglamento (UE) 2017/746([71]), excepto las entidades que fabrican

68 Reglamento (CE) n.º 1907/2006 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, relativo al registro, la evaluación, la autorización y la restricción de las sustancias y mezclas químicas (REACH), por el que se crea la Agencia Europea de Sustancias y Mezclas Químicas, se modifica la Directiva 1999/45/CE y se derogan el Reglamento (CEE) n.º 793/93 del Consejo y el Reglamento (CE) n.º 1488/94 de la Comisión, así como la Directiva 76/769/CEE del Consejo y las Directivas 91/155/CEE, 93/67/CEE, 93/105/CE y 2000/21/CE de la Comisión (DO L 396 de 30.12.2006, p. 1).

69 Reglamento (CE) n.º 178/2002 del Parlamento Europeo y del Consejo, de 28 de enero de 2002, por el que se establecen los principios y los requisitos generales de la legislación alimentaria, se crea la Autoridad Europea de Seguridad Alimentaria y se fijan procedimientos relativos a la seguridad alimentaria (DO L 31 de 1.2.2002, p. 1).

70 Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

71 Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico *in vitro* y por el que se derogan la Directiva 98/79/CE y la Decisión 2010/227/UE de la Comisión (DO L 117 de 5.5.2017, p. 176).

		productos sanitarios mencionadas en el anexo I, punto 5.
	b) Fabricación de productos informáticos, electrónicos y ópticos	Las empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 26, de la NACE Rev. 2
	c) Fabricación de material eléctrico	Las empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 27, de la NACE Rev. 2
	d) Fabricación de maquinaria y equipo n.c.o.p.	Las empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 28, de la NACE Rev. 2
	e) Fabricación de vehículos de motor, remolques y semirremolques	Las empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 29, de la NACE Rev. 2
	f) Fabricación de otro material de transporte	Las empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 30, de la NACE Rev. 2
6. Proveedores de servicios digitales		— Proveedores de mercados en línea
		— Proveedores de motores de búsqueda en línea
		— Proveedores de plataformas de servicios de redes sociales en línea