# DIRECTIVAS

## DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

**de 14 de diciembre de 2022**

**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) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)**

**(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 Banco Central Europeo ([1]),

Visto el dictamen del Comité Económico y Social Europeo ([2]),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario ([3]),

Considerando lo siguiente:

(1) El objetivo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([4]) era desarrollar las capacidades en materia de ciberseguridad en toda la Unión, reducir las amenazas para los sistemas de redes y de información utilizados para prestar servicios esenciales en sectores fundamentales, y garantizar la continuidad de dichos servicios en caso de incidentes, contribuyendo así a la seguridad de la Unión y al funcionamiento eficaz de su economía y su sociedad.

(2) Desde la entrada en vigor de la Directiva (UE) 2016/1148 se han logrado considerables progresos en el incremento del nivel de ciberresiliencia de la Unión. La revisión de dicha Directiva ha demostrado que ha servido de catalizador del enfoque institucional y normativo 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 de seguridad de los sistemas de redes y de información mediante la definición de estrategias nacionales de seguridad de los sistemas de redes y de información, el establecimiento de capacidades nacionales y la aplicación de medidas reguladoras que abarcan a las entidades y las infraestructuras esenciales determinadas por cada Estado miembro. Asimismo, la Directiva (UE) 2016/1148 ha propiciado la cooperación a nivel de la Unión mediante el establecimiento del Grupo de Cooperación y de la red de equipos de respuesta a incidentes de seguridad informática. A pesar de estos logros, la revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto algunas deficiencias inherentes que le impiden abordar eficazmente los retos actuales y emergentes en el ámbito de la ciberseguridad.

(3) Los sistemas de redes y de información se han convertido en un aspecto crucial 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 las ciberamenazas, 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 van en aumento y representan una grave amenaza para el funcionamiento de los sistemas de redes y de información. Como consecuencia de ello, los

([1]) DO C 233 de 16.6.2022, p. 22.
([2]) DO C 286 de 16.7.2021, p. 170.
([3]) Posición del Parlamento Europeo de 10 de noviembre de 2022 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 28 de noviembre de 2022.
([4]) 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).

incidentes pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, mermar 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. Además, la ciberseguridad es un factor facilitador esencial para que muchos sectores críticos se sumen con éxito a la transformación digital y aprovechen plenamente las ventajas económicas, sociales y sostenibles de la digitalización.

(4) La base jurídica de la Directiva (UE) 2016/1148 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 realizan actividades que son significativas desde el punto de vista económico varían considerablemente en función del Estado miembro por lo que respecta al tipo de requisitos, su nivel de detalle y el método de supervisión. Tales disparidades conllevan costes suplementarios y generan dificultades para las entidades 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 esas actividades transfronterizas. Además, es probable que una concepción o aplicación inadecuadas de los requisitos de ciberseguridad en un Estado miembro tenga repercusiones para el nivel de ciberseguridad de otros Estados miembros, máxime si se tiene en cuenta la intensidad de los intercambios transfronterizos. La revisión de la Directiva (UE) 2016/1148 ha puesto de manifiesto 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 que en ella se establecían. En consecuencia, dichas obligaciones venían aplicándose de manera considerablemente diferente en cada Estado miembro. También existen diferencias similares en la aplicación de las disposiciones de la Directiva (UE) 2016/1148 sobre supervisión y observancia.

(5) Todas esas diferencias conllevan una fragmentación del mercado interior y pueden tener efectos perjudiciales para su funcionamiento, afectando, en particular, a la prestación transfronteriza de servicios y al nivel de ciberresiliencia debido a la aplicación de medidas dispares. En última instancia, esas diferencias podrían derivar en una mayor vulnerabilidad de algunos Estados miembros frente a las ciberamenazas, cuyos efectos podrían sentirse en toda la Unión. El objetivo de la presente Directiva es eliminar estas divergencias tan pronunciadas entre los Estados miembros, concretamente mediante la definición de normas mínimas relativas al funcionamiento de un marco regulador coordinado, el establecimiento de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera eficaz, la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y la disponibilidad de vías de recurso y medidas de ejecución 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) Con la derogación de la Directiva (UE) 2016/1148, es preciso ampliar el ámbito de aplicación por sectores a una parte más extensa de la economía para ofrecer una cobertura completa de los sectores y servicios de vital importancia para las actividades sociales y económicas fundamentales dentro del mercado interior. En particular, la presente Directiva pretende tratar de superar las deficiencias de la diferenciación entre operadores de servicios esenciales y proveedores de servicios digitales, que ha quedado demostrado que es obsoleta al no reflejar la importancia de los sectores o servicios para las actividades sociales y económicas en el mercado interior.

(7) Con arreglo a la Directiva (UE) 2016/1148, los Estados miembros eran responsables de identificar las entidades que cumplían los criterios para ser consideradas operadores de servicios esenciales. A fin de eliminar las profundas divergencias entre los Estados miembros en ese sentido y garantizar la seguridad jurídica para todas las entidades pertinentes en lo que se refiere a las medidas para la gestión de riesgos de ciberseguridad 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 una norma sobre tamaño máximo con arreglo a la cual todas las entidades que sean consideradas medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión ([5]) o superen los límites máximos para las medianas

([5]) 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).

empresas previstos en el apartado 1 de dicho artículo y que operen en los sectores y presten el tipo de servicios o lleven a cabo las actividades a que se aplica la presente Directiva queden incluidas en su ámbito de aplicación. Los Estados miembros también deben disponer que determinadas pequeñas empresas y microempresas, tal como se definen en el artículo 2, apartados 2 y 3, de dicho anexo, que cumplan criterios específicos que pongan de manifiesto su papel clave para la sociedad, la economía o para determinados sectores o tipos de servicios, queden comprendidas en el ámbito de aplicación de la presente Directiva.

(8) La exclusión de las entidades de la Administración pública del ámbito de aplicación de la presente Directiva debe aplicarse a las entidades cuyas actividades se lleven a cabo principalmente en los ámbitos de la seguridad nacional, la seguridad pública, la defensa, o la garantía del cumplimiento de la ley, incluidas la prevención, investigación, detección y enjuiciamiento de infracciones penales. No obstante, las entidades de la Administración pública cuyas actividades solo estén relacionadas marginalmente con dichos ámbitos no deben quedar excluidas del ámbito de aplicación de la presente Directiva. A los efectos de la presente Directiva, se considera que las entidades con competencias reguladoras no realizan actividades en el ámbito de la garantía del cumplimiento de la ley y, por lo tanto, no quedan excluidas por ese motivo del ámbito de aplicación de la presente Directiva. Las entidades de la Administración pública establecidas conjuntamente con un tercer país conforme a un acuerdo internacional quedan excluidas del ámbito de aplicación de la presente Directiva. La presente Directiva no se aplica a las misiones diplomáticas y consulares de los Estados miembros en terceros países ni a sus sistemas de redes y de información, en la medida en que dichos sistemas estén situados en las dependencias de la misión o se utilicen para usuarios ubicados en un tercer país.

(9) Los Estados miembros deben tener la capacidad de adoptar las medidas necesarias para garantizar la protección de los intereses esenciales de seguridad nacional, preservar el orden público y la seguridad pública, y permitir la prevención, investigación, detección y enjuiciamiento de infracciones penales. A tal fin, los Estados miembros deben poder eximir a las entidades específicas que llevan a cabo actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley, incluidas las de prevención, investigación, detección y enjuiciamiento de infracciones penales, de determinadas obligaciones establecidas en la presente Directiva en relación con dichas actividades. Cuando una entidad preste servicios exclusivamente a una entidad de la Administración pública excluida del ámbito de aplicación de la presente Directiva, los Estados miembros deben poder eximir a dicha entidad de determinadas obligaciones establecidas en la presente Directiva en relación con dichos servicios. Además, ningún Estado miembro debe estar obligado a facilitar información cuya divulgación sea contraria a los intereses esenciales de su seguridad nacional, seguridad pública o defensa. Deben tenerse en cuenta a estos efectos las normas de la Unión o nacionales 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 (Protocolo TLP, por sus siglas en inglés). El Protocolo TLP debe entenderse como un medio para facilitar información sobre cualquier limitación de la difusión ulterior de la información. Se utiliza en casi todos los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) y en algunos centros de puesta en común y análisis de la información.

(10) Aunque la presente Directiva se aplica a las entidades que realizan actividades de producción de electricidad en centrales nucleares, algunas de esas actividades pueden tener vinculación con la seguridad nacional. En ese caso, los Estados miembros deben poder ejercer su responsabilidad de preservar la seguridad nacional con respecto a dichas actividades, incluidas las actividades dentro de la cadena de valor nuclear, de conformidad con los Tratados.

(11) Algunas entidades llevan a cabo actividades en el ámbito de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley, incluidas la prevención, investigación, detección y enjuiciamiento de infracciones penales, al tiempo que prestan servicios de confianza. Los prestadores de servicios de confianza incluidos en el ámbito de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([6]) deben estar comprendidos en el ámbito de aplicación de la presente Directiva a fin de garantizar el mismo nivel de requisitos de seguridad y supervisión que el establecido anteriormente en dicho Reglamento por lo que respecta a los prestadores de servicios de confianza. En consonancia con la exclusión de determinados servicios del Reglamento (UE) n.º 910/2014, la presente Directiva no debe aplicarse a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes.

([6]) 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).

(12) Los proveedores de servicios postales tal como se definen en la Directiva 97/67/CE del Parlamento Europeo y del Consejo ([7]), incluidos los proveedores de servicios de mensajería, deben estar sujetos a la presente Directiva si se ocupan de al menos una de las fases de la cadena de distribución postal y en particular de la recogida, la clasificación, el transporte o la distribución de envíos postales, incluida la recogida por el destinatario, teniendo en cuenta al mismo tiempo su grado de dependencia de los sistemas de redes y de información. Los servicios de transporte que no se lleven a cabo en combinación con alguna de esas fases deben quedar excluidos del ámbito de los servicios postales.

(13) Dada la intensificación y la mayor sofisticación de las ciberamenazas, los Estados miembros deben esforzarse por garantizar que las entidades excluidas del ámbito de aplicación de la presente Directiva alcancen un elevado nivel de ciberseguridad y por apoyar la aplicación de medidas equivalentes de gestión de riesgos de ciberseguridad que reflejen el carácter sensible de dichas entidades.

(14) El Derecho de la Unión en materia de protección de datos y de la intimidad se aplica a todo tratamiento de datos personales realizado en virtud de la presente Directiva. En particular, la presente Directiva se entiende sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([8]) y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([9]). Por consiguiente, la presente Directiva no debe afectar, en particular, a los cometidos y competencias de las autoridades competentes para supervisar el cumplimiento del Derecho de la Unión en materia de protección de datos y de la intimidad aplicables.

(15) Las entidades incluidas en el ámbito de aplicación de la presente Directiva a efectos del cumplimiento de las medidas para la gestión de riesgos de ciberseguridad deben clasificarse en dos categorías, entidades esenciales y entidades importantes, en función del grado de criticidad de sus sectores o del tipo de servicio que prestan, así como de su tamaño. A este respecto, deben tenerse debidamente en cuenta las correspondientes evaluaciones de riesgos sectoriales o las orientaciones de las autoridades competentes, en su caso. Se han de diferenciar los regímenes de supervisión y de garantía del cumplimiento de las dos categorías de entidades para garantizar un equilibrio justo entre los requisitos y las obligaciones en función del riesgo, por un lado, y la carga administrativa derivada de la supervisión del cumplimiento, por el otro.

(16) A fin de evitar que las entidades que tengan empresas asociadas o que sean empresas vinculadas se consideren entidades esenciales o importantes cuando ello sea desproporcionado, los Estados miembros deben tener la posibilidad de tomar en consideración el grado de independencia de que goza la entidad en relación con sus empresas asociadas o vinculadas al aplicar el artículo 6, apartado 2, del anexo de la Recomendación 2003/361/CE. En particular, los Estados miembros han de poder tener en cuenta el hecho de que una entidad sea independiente de sus empresas asociadas o vinculadas por lo que se refiere a los sistemas de redes y de información que dicha entidad utiliza para la prestación de sus servicios y en cuanto a los servicios que la entidad presta. Así, los Estados miembros deben poder tomar en consideración, en su caso, que la entidad no puede ser considerada mediana empresa con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE, o no supera los límites máximos para una mediana empresa que prevé el apartado 1 de dicho artículo si, tras tener en cuenta el grado de independencia de dicha entidad, no se consideraría como mediana empresa o que supera dichos límites máximos de haberse tenido en cuenta únicamente sus propios datos. Esto no afecta a las obligaciones que establece la presente Directiva incumben a las empresas asociadas y vinculadas incluidas en el ámbito de aplicación de la presente Directiva.

(17) Los Estados miembros han de poder decidir que las entidades que antes de la entrada en vigor de la presente Directiva eran consideradas operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 pasen a ser consideradas entidades esenciales.

---

([7]) 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).

([8]) 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).

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

(18) A fin de garantizar una visión clara de las entidades incluidas en el ámbito de aplicación de la presente Directiva, los Estados miembros deben elaborar una lista de las entidades esenciales e importantes así como de entidades que prestan servicios de registro de nombres de dominio. A tal fin, los Estados miembros deben exigir a las entidades que presenten, al menos, la siguiente información a las autoridades competentes, a saber, el nombre, la dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono de la entidad, y en su caso, el sector y subsector pertinente contemplados en los anexos, así como en su caso, una lista de los Estados miembros en los que prestan servicios incluidos en el ámbito de aplicación de la presente Directiva. A tal fin, la Comisión, asistida por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), debe proporcionar sin demora indebida orientaciones y modelos relativos a la obligación de presentar información. Para facilitar la elaboración y la actualización de la lista de entidades esenciales e importantes así como de las entidades que prestan servicios de registro de nombres de dominio, los Estados miembros deben poder establecer mecanismos nacionales para que las entidades se inscriban ellas mismas. Cuando existan registros a nivel nacional, los Estados miembros han de poder decidir los mecanismos adecuados que permitan determinar las entidades incluidas en el ámbito de aplicación de la presente Directiva.

(19) Los Estados miembros deben ser responsables de presentar a la Comisión, al menos, el número de entidades esenciales e importantes en cada sector y subsector contemplados en los anexos, así como información pertinente sobre el número de entidades identificadas y la disposición de la presente Directiva con arreglo a la cual se hayan identificado, y el tipo de servicio que prestan. Se alienta a los Estados miembros a intercambiar con la Comisión información sobre las entidades esenciales e importantes y, en caso de incidente de ciberseguridad a gran escala, información pertinente, como el nombre de la entidad afectada.

(20) La Comisión, en cooperación con el Grupo de Cooperación y tras consultar a las partes interesadas pertinentes, debe proporcionar directrices sobre la aplicación de los criterios aplicables a las microempresas y pequeñas empresas para evaluar si están comprendidas en el ámbito de la presente Directiva. Asimismo, la Comisión ha de asegurarse de que se ofrezcan orientaciones adecuadas a todas las microempresas y pequeñas empresas incluidas en el ámbito de aplicación de la presente Directiva. La Comisión, con el apoyo de los Estados miembros, debe proporcionar información al respecto a las microempresas y pequeñas empresas.

(21) La Comisión podría ofrecer orientaciones para ayudar a los Estados miembros a aplicar las disposiciones de la presente Directiva sobre su ámbito de aplicación y a evaluar la proporcionalidad de las medidas que se adopten en virtud de ella, en particular por lo que respecta a las entidades con modelos empresariales o entornos operativos de tal complejidad que una entidad pueda cumplir simultáneamente los criterios correspondientes a las entidades esenciales y a las importantes o realizar simultáneamente tanto actividades que quedan comprendidas en el ámbito de aplicación de la presente Directiva como actividades que quedan fuera de él.

(22) La presente Directiva constituye la base de referencia para las medidas para la 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 suplementarias relativas a las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación para garantizar un elevado nivel de ciberseguridad en toda la Unión, la Comisión ha de evaluar si dichas disposiciones podrían establecerse en un acto de ejecución adoptado con arreglo a la presente Directiva. En caso de que dicho acto de ejecución no se adecue a esa finalidad, los actos jurídicos sectoriales de la Unión podrían contribuir a garantizar un nivel elevado de ciberseguridad en toda la Unión, teniendo al mismo tiempo plenamente en cuenta las especificidades y complejidades de los sectores de que se trate. A tal fin, la presente Directiva no es óbice para que se adopten nuevos actos jurídicos sectoriales de la Unión que aborden las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación y que tengan debidamente en cuenta la necesidad de un marco de ciberseguridad global y coherente. La presente Directiva 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.

(23) Cuando un acto jurídico sectorial de la Unión incluya disposiciones que exijan a las entidades esenciales o importantes adoptar medidas para la gestión de riesgos de ciberseguridad o notificar los incidentes significativos y dichas obligaciones tengan un efecto al menos equivalente al de las obligaciones establecidas en la presente

Directiva, se deben aplicar a las mencionadas entidades tales disposiciones, incluidas las relativas a la supervisión y la ejecución. Si un acto jurídico sectorial de la Unión no comprende todas las entidades de un sector concreto incluidas en el ámbito de aplicación de la presente Directiva, las disposiciones pertinentes de la presente Directiva deben seguir aplicándose a las entidades no comprendidas en dicho acto.

(24) Cuando las disposiciones de un acto jurídico sectorial de la Unión exijan a las entidades esenciales o importantes que cumplan obligaciones de notificación de efecto al menos equivalente a las obligaciones de notificación establecidas en la presente Directiva, deben garantizarse la coherencia y la eficacia de la tramitación de las notificaciones de incidentes. A tal fin, las disposiciones del acto jurídico sectorial de la Unión sobre notificación de incidentes deben proporcionar a los CSIRT, autoridades competentes o puntos de contacto únicos sobre ciberseguridad (en lo sucesivo, «puntos de contacto únicos») designados con arreglo a la presente Directiva acceso inmediato a las notificaciones de incidentes presentadas de conformidad con el acto jurídico sectorial de la Unión. En particular, tal acceso inmediato puede garantizarse si las notificaciones de incidentes se transmiten sin demora indebida al CSIRT, la autoridad competente o el punto de contacto único con arreglo a la presente Directiva. En su caso, los Estados miembros deben establecer un mecanismo de notificación automática y directa que garantice un intercambio sistemático e inmediato de información con los CSIRT, las autoridades competentes o los puntos de contacto únicos en relación con la tramitación de dichas notificaciones de incidentes. A fin de simplificar la notificación y de aplicar el mecanismo de notificación automática y directa, los Estados miembros, de conformidad con el acto jurídico sectorial de la Unión, podrían utilizar un punto de entrada único.

(25) Los actos jurídicos sectoriales de la Unión que requieran medidas para la gestión de riesgos de ciberseguridad u obligaciones de notificación que sean de efecto al menos equivalente al de las establecidas en la presente Directiva podrían disponer que sus autoridades competentes con arreglo a dichos actos ejerzan sus facultades de supervisión y ejecución relativas a tales medidas u obligaciones con la asistencia de las autoridades competentes con arreglo a la presente Directiva. Las autoridades competentes de que se trate podrían establecer acuerdos de cooperación a tal fin. Tales 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, así como un mecanismo de intercambio de información pertinente en materia de supervisión y ejecución entre las autoridades competentes, que incluya acceso a la información sobre aspectos cibernéticos solicitada por las autoridades competentes con arreglo a la presente Directiva.

(26) Cuando los actos jurídicos sectoriales de la Unión exijan a las entidades que notifiquen ciberamenazas significativas, u ofrezcan incentivos para ello, los Estados miembros también deben fomentar la puesta en común de ciberamenazas significativas con los CSIRT, las autoridades competentes o los puntos de contacto únicos con arreglo a la presente Directiva, a fin de garantizar un mayor nivel de sensibilización de dichos organismos sobre el panorama de las ciberamenazas y permitirles responder de manera eficaz y rápida en caso de que se materialicen las ciberamenazas significativas.

(27) Los futuros actos jurídicos sectoriales de la Unión deben tener debidamente en cuenta las definiciones y el marco de supervisión y ejecución establecidos en la presente Directiva.

(28) El Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([10]) debe considerarse un acto jurídico de la Unión de carácter sectorial en relación con la presente Directiva por lo que respecta a las entidades financieras. En lugar de las disposiciones contempladas en la presente Directiva, deben aplicarse las disposiciones del Reglamento (UE) 2022/2554 relativas a las medidas de gestión de los riesgos de las tecnologías de la información y de las comunicaciones (TIC), la gestión de los incidentes relacionados con las TIC y, en particular, la notificación de incidentes graves relacionados con las TIC, así como las pruebas de la resiliencia operativa digital, los mecanismos de intercambio de información y los riesgos de terceros relacionados con las TIC. En consecuencia, los Estados miembros no deben aplicar a ninguna entidad financiera comprendida en el Reglamento (UE) 2022/2554 las disposiciones de la presente Directiva relativas a las obligaciones de gestión de los riesgos de ciberseguridad y de notificación y a la supervisión y la ejecución. Al mismo tiempo, es importante mantener una estrecha relación y el intercambio de información con el sector financiero en el marco de la presente Directiva. A tal fin, el Reglamento (UE) 2022/2554 permite a las Autoridades Europeas de Supervisión (AES) y a las autoridades competentes con arreglo a dicho Reglamento participar en las actividades del Grupo de Cooperación e intercambiar información y cooperar con los puntos de contacto únicos, así como con los CSIRT y las autoridades competentes designados en virtud de la presente Directiva. Las autoridades competentes a efectos del Reglamento (UE) 2022/2554 también

([10]) Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (véase la página 1 del presente Diario Oficial).

deben transmitir información detallada sobre los incidentes graves relacionados con las TIC y, en su caso, sobre las ciberamenazas significativas, a los CSIRT, las autoridades competentes o los puntos de contacto únicos designados en virtud de la presente Directiva. Esto se puede conseguir facilitando el acceso inmediato a las notificaciones de incidentes y transmitiéndolas bien de forma, bien a través de un punto de entrada único para la notificación de incidentes. Además, los Estados miembros deben seguir incluyendo al sector financiero en sus estrategias de ciberseguridad y los CSIRT pueden ocuparse del sector financiero en sus actividades.

(29) A fin de evitar lagunas y duplicaciones entre las obligaciones en materia de ciberseguridad impuestas a las entidades del sector de la aviación, las autoridades nacionales contempladas en los Reglamentos (CE) n.º 300/2008 ([11]) y (UE) 2018/1139 ([12]) del Parlamento Europeo y del Consejo y las autoridades competentes con arreglo a la presente Directiva deben cooperar con respecto a la aplicación de las medidas para la gestión de riesgos de ciberseguridad y la supervisión del cumplimiento de dichas medidas a escala nacional. Las autoridades competentes con arreglo a la presente Directiva podrían considerar que el cumplimiento por parte de una entidad de los requisitos de seguridad establecidos en los Reglamentos (CE) n.º 300/2008 y (UE) 2018/1139 y en los actos delegados y de ejecución pertinentes adoptados en virtud de dichos Reglamentos constituye un cumplimiento de los requisitos correspondientes establecidos en la presente Directiva.

(30) En vista de las interrelaciones que existen entre la ciberseguridad y la seguridad física de las entidades, debe garantizarse un enfoque coherente entre la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo ([13]) y la presente Directiva. Para ello, las entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557, deben ser consideradas entidades esenciales a los efectos de la presente Directiva. Asimismo, cada Estado miembro debe velar por que sus estrategias nacionales de ciberseguridad establezcan un marco de actuación para mejorar la coordinación dentro de dicho Estado miembro entre las autoridades competentes con arreglo a la presente Directiva y las competentes con arreglo a la Directiva (UE) 2022/2557 en el contexto del intercambio de información sobre los riesgos, ciberamenazas e incidentes relacionados con la ciberseguridad, así como sobre los riesgos, amenazas e incidentes no relacionados con la ciberseguridad, y sobre el ejercicio de las tareas de supervisión. Las autoridades competentes con arreglo a la presente Directiva y las que lo son con arreglo a la Directiva (UE) 2022/2557 deben cooperar e intercambiar información sin demora indebida, en particular en lo que se refiere a la identificación de las entidades críticas, los riesgos, las ciberamenazas e incidentes relacionados con la ciberseguridad, así como en lo que se refiere a los riesgos, amenazas e incidentes no relacionados con la ciberseguridad que afecten a las entidades críticas, incluidas las medidas de ciberseguridad y físicas adoptadas por las entidades críticas, así como en lo que se refiere a 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 con arreglo a la presente Directiva y las que lo son con arreglo a la Directiva (UE) 2022/2557 y de reducir al mínimo la carga administrativa de las entidades afectadas, dichas autoridades competentes deben esforzarse por armonizar los modelos de notificación de incidentes y los procesos de supervisión. En su caso, las autoridades competentes con arreglo a la Directiva (UE) 2022/2557 deben poder solicitar a las autoridades competentes con arreglo a la presente Directiva que ejerzan sus facultades de supervisión y ejecución respecto a una entidad que esté identificada como entidad crítica con arreglo a la Directiva (UE) 2022/2557 A tal fin, las autoridades competentes con arreglo a la presente Directiva y las que lo son con arreglo a la Directiva (UE) 2022/2557 deben cooperar e intercambiar información, en tiempo real siempre que sea posible.

(31) Las entidades pertenecientes al sector de las infraestructuras digitales se basan esencialmente en sistemas de redes y 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 medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación. Dado que esas cuestiones entran en el ámbito de aplicación de la presente Directiva, las obligaciones establecidas en los capítulos III, IV y VI de la Directiva (UE) 2022/2557 no se aplican a dichas entidades.

([11]) 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).

([12]) 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).

([13]) Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva del Consejo 2008/114/CE (véase la página 164 del presente Diario Oficial).

(32) El mantenimiento y la conservación de un sistema de nombres de dominio (DNS, por sus siglas en inglés) fiable, resiliente y seguro son factores fundamentales para garantizar la integridad de internet y resultan cruciales para que funcione con estabilidad y de manera ininterrumpida, de lo que depende la economía digital y la sociedad. Por consiguiente, la presente Directiva ha de aplicarse a los registros de nombres de dominio de primer nivel, así como a los proveedores de servicios de DNS que deban considerarse entidades prestadoras de servicios de resolución recursiva de nombres de dominio para usuarios finales de internet o servicios de resolución autoritativa de nombres de dominio para uso de terceros. La presente Directiva no debe aplicarse a los servidores raíz.

(33) Los servicios de computación en nube deben abarcar los servicios digitales que permiten la administración bajo demanda y el acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos que se pueden compartir, también cuando esos recursos están distribuidos entre varias ubicaciones. Entre tales recursos se encuentran 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, por sus siglas en inglés), la plataforma como servicio (PaaS, por sus siglas en inglés), el software como servicio (SaaS, por sus siglas en inglés) y la red como servicio (NaaS, por sus siglas en inglés). Los modelos de despliegue de la computación en nube deben incluir las nubes privadas, comunitarias, públicas e híbridas. Los modelos de servicio y despliegue de la computación en nube 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 a través de 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 y estaciones de trabajo. El término «modulable» se refiere a los recursos informáticos que el proveedor de servicios en nube asigna de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término «conjunto elástico» se usa para describir los recursos informáticos que se movilizan y liberan 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 cuyo tratamiento se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico. El término «distribuidos» 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.

(34) Habida cuenta de la aparición de tecnologías innovadoras y nuevos modelos de negocio, se espera que surjan en el mercado interior nuevos modelos de despliegue y servicios 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»).

(35) Los servicios ofrecidos por los proveedores de servicios de centro de datos no siempre se prestan en forma de servicio de computación en nube. En consecuencia, los centros de datos no siempre forman parte de una infraestructura de computación en nube. A fin de gestionar todos los riesgos que se plantean para la seguridad de los sistemas de redes y de información, la presente Directiva debe aplicarse a los proveedores de estos servicios de centro de datos que no sean 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 engloba las estructuras, o las agrupaciones de estructuras, dedicadas al alojamiento, la interconexión y la explotación centralizados de tecnologías de la información y equipos de red que presten 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 debe aplicarse a los centros de datos empresariales internos cuya propiedad y explotación para fines propios corresponden a la entidad de que se trate.

(36) Las actividades de investigación son fundamentales en el desarrollo de nuevos productos y procesos. Muchas de esas actividades son realizadas por entidades que comparten, difunden o aprovechan los resultados de su investigación con fines comerciales. En consecuencia, esas entidades pueden ser eslabones importantes de las cadenas de valor, por lo que la seguridad de sus sistemas de redes y de información es parte integrante de la ciberseguridad global del mercado interior. Debe entenderse que entre los organismos de investigación están incluidas las entidades que

dedican la parte esencial de sus actividades a la investigación aplicada o al desarrollo experimental, en el sentido del Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental, de la Organización de para la Cooperación y el Desarrollo Económicos, con el propósito de aprovechar sus resultados con fines comerciales, como la fabricación o desarrollo de un producto, proceso o la prestación de un servicio, o su comercialización.

(37) Las crecientes interdependencias son el resultado de una red cada vez más transfronteriza e interdependiente de prestación de servicios que utilizan infraestructuras clave de toda la Unión en sectores como la energía, el transporte, la infraestructura digital, el agua potable y las aguas residuales, la sanidad y determinados aspectos de la administración pública, así como el espacio en la medida en que se trate de la prestación de determinados servicios que dependen de infraestructuras terrestres cuya propiedad, gestión y explotación corresponden a los Estados miembros o entidades privadas, quedando al margen, por tanto, las infraestructuras cuya propiedad, gestión u explotación corresponden a la Unión o a terceros en su nombre como parte de su programa espacial. Esas 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 ocasionar repercusiones de gran alcance y duración en la prestación de servicios en todo el mercado interior. La intensificación de los ciberataques durante la pandemia de COVID-19 han puesto de relieve la vulnerabilidad de unas sociedades cada vez más interdependientes frente a riesgos de baja probabilidad.

(38) 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 o crear una o varias autoridades nacionales competentes encargadas de la ciberseguridad y de los cometidos de supervisión previstos en la presente Directiva.

(39) 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 que se encargue de coordinar las cuestiones relacionadas con la seguridad de los sistemas de redes y de información y de la cooperación transfronteriza a escala de la Unión.

(40) Los puntos de contacto únicos deben garantizar la eficacia de la cooperación transfronteriza con las autoridades pertinentes de otros Estados miembros y, en su caso, con la Comisión y la ENISA. Por consiguiente, los puntos de contacto únicos deben encargarse de transmitir las notificaciones de incidentes significativos con impacto transfronterizo a los puntos de contacto únicos de otros Estados miembros afectados a petición del CSIRT o de la autoridad competente. A nivel nacional, los puntos de contacto únicos deben permitir una cooperación intersectorial fluida con otras autoridades competentes. Los puntos de contacto únicos también podrían ser los destinatarios de la información pertinente sobre incidentes relativos a entidades financieras remitida por las autoridades competentes con arreglo al Reglamento (UE) 2022/2554, que deben poder transmitir, según proceda, a los CSIRT o a las autoridades competentes designados con arreglo a la presente Directiva.

(41) Los Estados miembros deben estar debidamente equipados, tanto en términos de capacidades técnicas como de capacidades organizativas, para las labores de prevención, detección, respuesta ante incidentes y riesgos y para reducirlos. Por consiguiente, los Estados miembros deben crear o designar uno o varios CSIRT con arreglo a la presente Directiva y velar por que dispongan de recursos y capacidades técnicas adecuados. Los CSIRT deben cumplir los requisitos establecidos en la presente Directiva para garantizar las capacidades efectivas y compatibles que permitan hacer frente a incidentes y riesgos y lograr una cooperación eficaz a escala de la Unión. Los Estados miembros deben poder designar como CSIRT a equipos de respuesta a emergencias informáticas (CERT, por sus siglas en inglés) ya existentes. 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 deben poder considerar la posibilidad de establecer una separación funcional entre las funciones 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.

(42) Los CSIRT se encargan de la gestión de incidentes, lo que implica el tratamiento de grandes volúmenes de datos a veces sensibles. Los Estados miembros deben garantizar que los CSIRT cuenten con infraestructura para el intercambio y el tratamiento de información, así como con personal debidamente equipado, de modo que se garantice la confidencialidad y fiabilidad de sus operaciones. Los CSIRT también podrían adoptar códigos de conducta a ese respecto.

(43) Por lo que respecta a los datos personales, los CSIRT deben poder ofrecer, con arreglo al Reglamento (UE) 2016/679 y a petición de una entidad esencial o importante, una exploración proactiva de los sistemas de redes y de información utilizados por dicha entidad para la prestación de sus servicios. Cuando proceda, los Estados miembros deben tratar de garantizar el mismo nivel de capacidades técnicas para todos los CSIRT sectoriales. Los Estados miembros deben poder solicitar la asistencia de la ENISA a la hora de desarrollar sus CSIRT.

(44) Los CSIRT han de tener la capacidad, a petición de una entidad esencial o importante, de realizar un seguimiento de los activos expuestos a internet de dicha entidad, tanto dentro como fuera de sus instalaciones, a fin de detectar, comprender y gestionar los riesgos organizativos generales de la entidad por lo que se refiere a los riesgos o vulnerabilidades críticas de la cadena de suministro recientemente detectados. Debe alentarse a la entidad a comunicar al CSIRT si opera una interfaz de gestión privilegiada, ya que esta circunstancia podría afectar a la rapidez de emprender acciones de reducción de riesgos.

(45) 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, a efectos del desempeño de sus funciones, los CSIRT y las autoridades competentes deben poder intercambiar información, incluidos datos personales, con equipos nacionales de respuesta a incidentes de seguridad informática o autoridades competentes de terceros países, siempre que se cumplan las condiciones establecidas en el Derecho de la Unión en materia de protección de datos para las transferencias de datos personales a terceros países, entre otras las del artículo 49 del Reglamento (UE) 2016/679.

(46) Es esencial garantizar recursos adecuados para cumplir los objetivos de la presente Directiva y permitir que las autoridades competentes y los CSIRT puedan llevar a cabo los cometidos aquí encomendados. Los Estados miembros pueden introducir a nivel nacional un mecanismo de financiación para cubrir los gastos necesarios en relación con el desempeño de las funciones de las entidades públicas encargadas de la ciberseguridad en el Estado miembro con arreglo a la presente Directiva. Dicho mecanismo debe cumplir el Derecho de la Unión, ser proporcionado y no discriminatorio, y debe tener en cuenta diferentes enfoques para la prestación de servicios seguros.

(47) La red de CSIRT debe seguir contribuyendo a reforzar la confianza y la seguridad y a promover una cooperación operativa rápida y eficaz entre los Estados miembros. Con vistas a reforzar la cooperación operativa a escala de la Unión, la red de CSIRT debe considerar la posibilidad de invitar a que participen en sus actividades los órganos y organismos de la Unión implicados en la política de ciberseguridad, como Europol.

(48) Con el fin de alcanzar y mantener un elevado nivel de ciberseguridad, las estrategias nacionales de ciberseguridad exigidas con arreglo a la presente Directiva deben consistir en marcos coherentes que establezcan prioridades y objetivos estratégicos en el ámbito de la ciberseguridad, así como la gobernanza para alcanzarlos. Tales estrategias pueden consistir en uno o varios instrumentos legislativos o no legislativos.

(49) Las políticas de ciberhigiene proporcionan la base para proteger la seguridad de las infraestructuras de los sistemas de redes y de información, del hardware, del software y de las aplicaciones en línea, así como los datos comerciales o de usuarios finales de los que dependen las entidades. Las políticas de ciberhigiene, que comprenden un conjunto básico común de prácticas, como las actualizaciones de software y hardware, los cambios de contraseña, la gestión de la instalación de software nuevo, la limitación de las cuentas con acceso de nivel administrador y las copias de seguridad de datos, permiten establecer un marco proactivo de preparación y seguridad global en caso de incidentes o ciberamenazas. La ENISA debe supervisar y analizar las políticas de ciberhigiene de los Estados miembros.

(50) La sensibilización en materia de ciberseguridad y la ciberhigiene son esenciales para mejorar el nivel de ciberseguridad dentro de la Unión, en particular a la luz del creciente número de dispositivos conectados que cada vez con más frecuencia se usan en los ciberataques. Deben realizarse esfuerzos para aumentar la sensibilización general sobre los riesgos relacionados con dichos dispositivos, mientras que las evaluaciones a escala de la Unión podrían contribuir a garantizar una comprensión común de dichos riesgos en el mercado interior.

(51) Los Estados miembros deben fomentar el uso de toda tecnología innovadora, incluida la inteligencia artificial, cuyo uso pueda mejorar la detección y la prevención de ciberataques, permitiendo que los recursos se desvíen de manera más eficaz hacia la lucha contra los ciberataques. Por consiguiente, los Estados miembros deben promover en sus estrategias nacionales de ciberseguridad las actividades de investigación y desarrollo encaminadas a facilitar el uso de dichas tecnologías, en particular las relativas a herramientas automatizadas o semiautomatizadas en materia de ciberseguridad, y, en su caso, el intercambio de datos necesarios para formar a los usuarios de esas tecnologías y mejorarlas. El uso de cualquier tecnología innovadora, incluida la inteligencia artificial, debe cumplir el Derecho de la Unión en materia de protección de datos, incluidos los principios de protección de datos de exactitud, minimización de datos, equidad y transparencia, y de seguridad de datos, como el cifrado avanzado. Los requisitos de protección de datos desde el diseño y por defecto establecidos en el Reglamento (UE) 2016/679 deben aprovecharse al máximo.

(52) Las herramientas y aplicaciones de ciberseguridad de código abierto pueden contribuir a un mayor grado de apertura y repercutir positivamente en la eficiencia de la innovación industrial. Unos estándares abiertos facilitan la interoperabilidad entre herramientas de seguridad, contribuyendo así a la seguridad de las partes interesadas de la industria. Las herramientas y aplicaciones de ciberseguridad de código abierto pueden suponer un impulso para la amplia comunidad de desarrolladores, permitiendo la diversificación de los proveedores. El código abierto puede propiciar un proceso de verificación más transparente de las herramientas relacionadas con la ciberseguridad y un proceso de detección de vulnerabilidades a cargo de la comunidad. Por consiguiente, los Estados miembros deben poder promover el uso de software de código abierto y estándares abiertos mediante la aplicación de políticas relativas al uso de datos abiertos y de código abierto como parte de la estrategia de seguridad a través de la transparencia. Las políticas que promueven la introducción y el uso sostenible de herramientas de ciberseguridad de código abierto revisten especial importancia para las pequeñas y medianas empresas que se enfrentan a costes significativos de implementación, costes que pueden reducirse al mínimo si también se reduce la necesidad de aplicaciones o herramientas específicas.

(53) Los servicios públicos básicos están cada vez más conectados a las redes digitales de las ciudades, con el fin de reforzar las redes de transporte urbano, mejorar el suministro de agua y las instalaciones de eliminación de residuos y aumentar la eficiencia del alumbrado y de la calefacción de los edificios. Dichos servicios públicos básicos digitalizados son vulnerables a los ciberataques y corren el riesgo, en caso de éxito de un ciberataque, de causar daños en gran escala a los ciudadanos debido a su interconexión. Los Estados miembros deben desarrollar una política que aborde el desarrollo de tales ciudades conectadas o inteligentes, y sus posibles efectos en la sociedad, como parte de su estrategia nacional de ciberseguridad.

(54) En los últimos años, la Unión se ha enfrentado a un aumento exponencial de los ataques con programas de secuestro («ramsonware»), en los que los programas maliciosos cifran datos y sistemas y exigen el pago de un rescate para liberarlos. La frecuencia y gravedad crecientes de los ataques con programas de secuestro pueden deberse a varios factores, como los distintos patrones de ataque, los modelos de negocio delictivos en torno a los «programas de secuestro como servicio» y las criptomonedas, la exigencia de rescates y el aumento de los ataques a las cadenas de suministro. Los Estados miembros deben adoptar una política para luchar contra el auge de los ataques con programas de secuestro como parte de sus estrategias nacionales de ciberseguridad.

(55) Las asociaciones entre el sector público y el privado en el ámbito de la ciberseguridad pueden ofrecer un marco adecuado para el intercambio de conocimientos y de buenas prácticas, así como para el establecimiento de un nivel común de entendimiento entre las partes interesadas. Los Estados miembros deben promover políticas que apoyen la creación de asociaciones público-privadas específicas en materia de ciberseguridad. Tales políticas deben precisar, entre otros aspectos, el alcance y las partes interesadas implicadas, el modelo de gobernanza, las opciones de financiación disponibles y la interacción entre las partes interesadas participantes en relación con las asociaciones público-privadas. Dichas asociaciones pueden aprovechar la experiencia de las entidades del sector privado para prestar ayuda a las autoridades competentes en el desarrollo de los servicios y procesos más avanzados, como el intercambio de información, las alertas tempranas, los ejercicios de ciberamenazas e incidentes, la gestión de crisis y la planificación de la resiliencia.

(56) Los Estados miembros, en sus estrategias nacionales de ciberseguridad, deben abordar las necesidades específicas de ciberseguridad de las pequeñas y medianas empresas. Las pequeñas y medianas empresas representan, en toda la Unión, un gran porcentaje del mercado industrial y empresarial, y a menudo tienen dificultades para adaptarse a las nuevas prácticas empresariales en un mundo más conectado y al entorno digital, con trabajadores que trabajan desde casa y negocios que cada vez con más frecuencia se realizan en línea. Algunas pequeñas y medianas empresas se enfrentan a retos específicos en materia de ciberseguridad como los escasos conocimientos sobre el ciberespacio, la falta de seguridad informática a distancia, el elevado coste de las soluciones de ciberseguridad y un mayor nivel de amenazas, como los programas de secuestro, para los que deberían recibir orientación y asistencia. Las pequeñas y medianas empresas cada vez sufren más ataques contra las cadenas de suministro debido al menor rigor de sus medidas para la gestión de riesgos de ciberseguridad y de su gestión de los ataques, y al hecho de que tienen unos recursos de seguridad limitados. Tales ataques a las cadenas de suministro no solo afectan a las pequeñas y medianas

empresas y sus operaciones de forma aislada, sino que también pueden tener un efecto en cascada en el marco de ataques más importantes contra las entidades a las que han suministrado. Los Estados miembros, por medio de sus estrategias nacionales de ciberseguridad, deben ayudar a las pequeñas y medianas empresas a hacer frente a los retos a los que se enfrentan en sus cadenas de suministro. Los Estados miembros deben contar con un punto de contacto para las pequeñas y medianas empresas a nivel nacional o regional que proporcione orientación y asistencia a las pequeñas y medianas empresas o las dirija a los organismos adecuados para que les proporcionen orientación y asistencia acerca de cuestiones relacionadas con la ciberseguridad. Se alienta asimismo a los Estados miembros a que ofrezcan servicios como la configuración de sitios web y la habilitación de registros a las microempresas y pequeñas empresas que carezcan de esas capacidades.

(57) En el marco de sus estrategias nacionales de ciberseguridad, los Estados miembros deben adoptar políticas de fomento de la ciberprotección activa como parte de una estrategia de defensa más amplia. A diferencia de las respuestas reactivas, la ciberprotección activa es la prevención, la detección, la supervisión, el análisis y la mitigación de los fallos de seguridad de la red de forma activa, en combinación con el uso de capacidades desplegadas dentro y fuera de la red víctima de los fallos. Podría incluir la oferta por parte de los Estados miembros de herramientas o servicios gratuitos a determinadas entidades, como controles de autoservicio, herramientas de detección y servicios de retirada. La capacidad de compartir y comprender de forma rápida y automática la información y el análisis de amenazas, las alertas de ciberactividad y las acciones de respuesta es crucial para que se puedan aunar los esfuerzos encaminados a prevenir, detectar, abordar y bloquear con éxito los ataques contra los sistemas de redes y de información. La ciberprotección activa se basa en una estrategia defensiva que excluye las medidas ofensivas.

(58) Puesto que la explotación de las vulnerabilidades de los sistemas de redes y de información puede causar perturbaciones y daños considerables, la determinación y subsanación rápidas de dichas vulnerabilidades son factores importantes para reducir los riesgos. Por consiguiente, las entidades que desarrollen o administren sistemas de redes y de información deben establecer procedimientos apropiados para abordar las vulnerabilidades cuando se detecten. Dado que las vulnerabilidades suelen ser detectadas y divulgadas por terceros, los fabricantes o proveedores de productos o servicios de TIC también deben establecer los procedimientos necesarios para recibir de terceros información sobre las vulnerabilidades. En este sentido, las normas internacionales ISO/IEC 30111 e ISO/IEC 29147 ofrecen orientación sobre la gestión y la divulgación de las vulnerabilidades. Reforzar la coordinación entre las personas físicas o jurídicas notificantes y los fabricantes o proveedores de productos o servicios de TIC reviste una gran importancia a la hora de facilitar un marco voluntario para la divulgación de vulnerabilidades. La divulgación coordinada de las vulnerabilidades se refiere específicamente a un proceso estructurado a través del cual las vulnerabilidades se notifican al fabricante o proveedor de los productos o servicios de TIC potencialmente vulnerables de manera que este pueda diagnosticar y subsanar las vulnerabilidades antes de que se divulgue información detallada a terceros o al público. Asimismo, la divulgación coordinada de las vulnerabilidades debe también comprender la coordinación entre la persona física o jurídica notificante y el fabricante o proveedor de los productos o servicios de TIC potencialmente vulnerables en lo tocante al momento de la subsanación y la publicación de las vulnerabilidades.

(59) La Comisión, la ENISA y los Estados miembros deben continuar promoviendo la alineación con las normas internacionales y las mejores prácticas existentes en la industria en el ámbito de la gestión de riesgos de ciberseguridad, por ejemplo en cuestiones como la evaluación de la seguridad de las cadenas de suministro, el intercambio de información y la divulgación de vulnerabilidades.

(60) Los Estados miembros, en cooperación con la ENISA, 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 al Derecho nacional. Dado que las personas físicas y jurídicas que investigan vulnerabilidades podrían incurrir en algunos Estados miembros en responsabilidad civil y penal, se alienta a los Estados miembros a que adopten directrices para que no se actúe penalmente cuando se trate de investigadores de seguridad de la información y que no se exija responsabilidad civil por sus actividades.

(61) Los Estados miembros deben designar uno de sus CSIRT como coordinador para que ejerza de intermediario entre las personas físicas o jurídicas notificantes y los fabricantes o proveedores de productos o servicios de TIC que puedan verse afectados por la vulnerabilidad, cuando sea necesario. Los cometidos del CSIRT designado como coordinador deben consistir, en particular, en identificar y contactar a las entidades afectadas, prestar asistencia a las personas físicas o jurídicas que notifican una vulnerabilidad, negociar los plazos de divulgación y gestionar las

vulnerabilidades que afectan a múltiples entidades (divulgación coordinada de las vulnerabilidades con múltiples interesados). Cuando la vulnerabilidad notificada pueda afectar de manera significativa a entidades en más de un Estado miembro, los CSIRT designados como coordinadores deben cooperar, en su caso, en el marco de la red de CSIRT.

(62) El acceso a información correcta y oportuna sobre las vulnerabilidades que afectan a productos y servicios de TIC contribuye a reforzar la gestión de los riesgos de ciberseguridad. Las fuentes de información sobre vulnerabilidades que se encuentran a disposición pública son una herramienta importante para las entidades y los usuarios de sus servicios, pero también para las autoridades competentes y los CSIRT. Por ese motivo, la ENISA debe crear una base de datos europea de vulnerabilidades en la que las entidades, con independencia de si quedan o no comprendidas en el ámbito de aplicación de la presente Directiva, y sus proveedores de sistemas de redes y de información, así como las autoridades competentes y los CSIRT, puedan divulgar y registrar, de manera voluntaria, las vulnerabilidades conocidas públicamente a fin de que los usuarios puedan adoptar las medidas de mitigación apropiadas. La finalidad de esa base de datos es abordar los singulares desafíos que plantean los riesgos para las entidades de la Unión. Además, la ENISA debe establecer un procedimiento adecuado para el proceso de publicación, a fin de dar a las entidades tiempo para adoptar medidas de mitigación en lo que respecta a sus vulnerabilidades, y emplear medidas avanzadas para la gestión de riesgos de ciberseguridad, así como conjuntos de datos legibles por máquina y las interfaces correspondientes. A fin de fomentar una cultura de divulgación de vulnerabilidades, la divulgación no debe tener efectos perjudiciales para la persona física o jurídica notificante.

(63) Aunque existen registros o bases de datos similares para las vulnerabilidades, su alojamiento y mantenimiento dependen de entidades que no están establecidas en la Unión. Con una base de datos europea de vulnerabilidades mantenida por la ENISA se conseguiría mejorar la transparencia del proceso de publicación antes de que la vulnerabilidad se divulgue públicamente y la resiliencia en caso de perturbación o interrupción en la prestación de servicios similares. A fin de evitar, en la medida de lo posible, la duplicación de esfuerzos y de buscar la complementariedad, la ENISA debe estudiar la posibilidad de celebrar acuerdos de cooperación estructurada con registros o bases de datos similares bajo jurisdicción de un tercer país. En particular, la ENISA debe estudiar la posibilidad de cooperar estrechamente con los operadores del sistema de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés).

(64) El Grupo de Cooperación debe apoyar y facilitar la cooperación estratégica y el intercambio de información, así como reforzar la confianza entre los Estados miembros. El Grupo de Cooperación debe elaborar un programa de trabajo cada dos años en el que se incluyan las acciones que ha de llevar a cabo el Grupo de Cooperación para llevar a la práctica sus objetivos y cometidos. El calendario para la elaboración del primer programa de trabajo adoptado con arreglo a la presente Directiva debe adecuarse al del último programa adoptado con arreglo a la Directiva (UE) 2016/1148, a fin de evitar posibles perturbaciones en el trabajo del Grupo de Cooperación.

(65) A la hora de elaborar documentos de orientación, el Grupo de Cooperación debe, de manera sistemática, cartografiar las soluciones y experiencias nacionales, evaluar el impacto de los resultados del Grupo de Cooperación en los enfoques nacionales, debatir los desafíos en materia de aplicación y formular recomendaciones específicas, en particular para facilitar la alineación de la transposición de la presente Directiva entre los Estados miembros, que deben abordarse mediante la mejora de la aplicación de las normas vigentes. El Grupo de Cooperación también podría mapear las soluciones nacionales para promover la compatibilidad de las soluciones de ciberseguridad aplicadas a cada sector específico en toda la Unión. Esto es especialmente importante en el caso de los sectores que tienen un carácter internacional y transfronterizo.

(66) El Grupo de Cooperación debe seguir siendo un foro flexible capaz de responder a las nuevas prioridades y desafíos estratégicos, teniendo en cuenta al mismo tiempo la disponibilidad de los recursos. Podría organizar reuniones conjuntas periódicas con partes interesadas privadas pertinentes de toda la Unión para tratar las actividades realizadas por el Grupo de Cooperación y recabar datos y apreciaciones sobre los desafíos estratégicos emergentes. Además, el Grupo de Cooperación debe llevar a cabo una evaluación periódica de la situación de las ciberamenazas o incidentes, como los programas de secuestro. Con vistas a reforzar la cooperación a escala de la Unión, el Grupo de Cooperación debe considerar la posibilidad de invitar a que participen en sus actividades las instituciones,

órganos y organismos pertinentes de la Unión implicados en la política de ciberseguridad, como el Parlamento Europeo, Europol, el Comité Europeo de Protección de Datos, la Agencia de la Unión Europea para la Seguridad Aérea, creada mediante el Reglamento (UE) 2018/1139, y la Agencia de la Unión Europea para el Programa Espacial, creada mediante el Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo ([14]).

(67) Las autoridades competentes y los CSIRT deben estar capacitados para participar en programas de intercambio para funcionarios de otros Estados miembros, dentro de un marco específico y, en su caso, a condición de que los funcionarios que participen en esos programas de intercambio cuenten con la habilitación de seguridad necesaria, con el fin de mejorar la cooperación y fortalecer la confianza entre los Estados miembros. 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 o el CSIRT de acogida.

(68) Los Estados miembros deben contribuir al establecimiento del Marco de respuesta a las crisis de ciberseguridad de la UE descrito en la Recomendación (UE) 2017/1584 de la Comisión ([15]) a través de las redes de cooperación existentes, en particular la Red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad (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 concreten los detalles de dicha cooperación y eviten la duplicación de tareas. El reglamento interno de la EU-CyCLONe debe especificar con mayor detalle las disposiciones por las que debe regirse el funcionamiento de esa red, incluidas las funciones de la red, los medios de cooperación, las interacciones con otros actores pertinentes y los modelos para el intercambio de información, así como los canales de comunicación. De cara a la gestión de crisis a escala de la Unión, las partes pertinentes deben recurrir al dispositivo de la UE de respuesta política integrada a las crisis con arreglo a la Decisión de Ejecución (UE) 2018/1993 del Consejo ([16]) (en lo sucesivo, «Dispositivo 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 exterior o de política común de seguridad y defensa, debe activarse el Mecanismo de Respuesta a las Crisis del Servicio Europeo de Acción Exterior.

(69) De conformidad con el anexo de la Recomendación (UE) 2017/1584, por incidente de ciberseguridad 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 de ciberseguridad a gran escala pueden intensificarse y convertirse en una crisis propiamente dicha que impida el correcto funcionamiento del mercado interior o plantee graves riesgos para la seguridad y la protección públicas de las entidades o los ciudadanos de varios Estados miembros o del conjunto de la Unión. 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 correctamente la respuesta en toda la Unión.

(70) Los incidentes de ciberseguridad a gran escala y las crisis en el ámbito de la Unión requieren una acción coordinada que garantice una respuesta rápida y eficaz, debido al elevado grado de interdependencia entre sectores y Estados miembros. La disponibilidad de sistemas de redes y de información ciberresilientes y la disponibilidad, confidencialidad e integridad de los datos son vitales para la seguridad de la Unión y para la protección de sus ciudadanos, empresas e instituciones frente a incidentes y ciberamenazas, así como para aumentar la confianza de las personas y organizaciones en la capacidad de la Unión de promover y proteger un ciberespacio mundial, abierto, libre, estable y seguro basado en los derechos humanos, las libertades fundamentales, la democracia y el Estado de Derecho.

([14]) Reglamento (UE) 2021/696 del Parlamento Europeo y del Consejo, de 28 de abril de 2021, por el que se crean el Programa Espacial de la Unión y la Agencia de la Unión Europea para el Programa Espacial y por el que se derogan los Reglamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 y (UE) n.º 377/2014 y la Decisión n.º 541/2014/UE (DO L 170 de 12.5.2021, p. 69).

([15]) 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).

([16]) Decisión de Ejecución (UE) 2018/1993 del Consejo, de 11 de diciembre de 2018, sobre el dispositivo de la UE de respuesta política integrada a las crisis (DO L 320 de 17.12.2018, p. 28).

(71) La EU-CyCLONe debe servir de intermediario entre los niveles técnico y político durante los incidentes y crisis de ciberseguridad a gran escala, y debe reforzar la cooperación a nivel operativo y apoyar la toma de decisiones a nivel político. En cooperación con la Comisión, habida cuenta de las competencias de la Comisión en el ámbito de la gestión de crisis, la EU-CyCLONe debe basarse en las conclusiones de la red de CSIRT y utilizar sus propias capacidades para elaborar análisis del impacto de los incidentes y crisis de ciberseguridad a gran escala.

(72) Los ciberataques son de carácter transfronterizo y un incidente significativo puede perturbar y dañar infraestructuras críticas de información de las que depende el buen funcionamiento del mercado interior. La Recomendación (UE) 2017/1584 aborda el papel de todos los actores pertinentes. Además, la Comisión es responsable, en el marco del Mecanismo de Protección Civil de la Unión establecido por la Decisión 1313/2013/UE del Parlamento Europeo y del Consejo ([17]), de las acciones generales de preparación, incluida la gestión del Centro de Coordinación de la Respuesta a Emergencias y del Sistema Común de Comunicación e Información de Emergencia, el mantenimiento y el desarrollo ulterior de las capacidades de conciencia y análisis situacionales, y el establecimiento y gestión de la capacidad de movilizar y enviar equipos de expertos en caso de solicitud de asistencia de un Estado miembro o de un tercer país. Asimismo la Comisión es responsable de proporcionar informes analíticos para el Dispositivo RPIC en virtud de la Decisión de Ejecución (UE) 2018/1993, también en relación con la conciencia situacional y la preparación en materia de ciberseguridad, así como con la conciencia situacional y la respuesta a las crisis en los ámbitos de la agricultura, las condiciones meteorológicas adversas, la cartografía y las previsiones de conflictos, los sistemas de alerta temprana de catástrofes naturales, las emergencias sanitarias, la vigilancia de las enfermedades infecciosas, la fitosanidad, los incidentes químicos, la seguridad de los alimentos y los piensos, la salud animal, la migración, las aduanas, las emergencias nucleares y radiológicas, y la energía.

(73) De conformidad con el artículo 218 del TFUE, la Unión puede celebrar, en su caso, acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen la participación de estos en determinadas actividades del Grupo de Cooperación, la red de CSIRT y la EU-CyCLONe. Dichos acuerdos deben velar por los intereses de la Unión y por una protección de datos adecuada. Esto no debe ser óbice para que los Estados miembros ejerzan su derecho a cooperar con terceros países afines en la gestión de vulnerabilidades y la gestión de riesgos en materia de ciberseguridad, facilitando la presentación de informes y el intercambio general de información de conformidad con el Derecho de la Unión.

(74) A fin de facilitar la aplicación efectiva de la presente Directiva en lo que se refiere, entre otros aspectos, a la gestión de las vulnerabilidades, medidas para la gestión de los riesgos de ciberseguridad, las obligaciones de notificación y los mecanismos de intercambio de información sobre ciberseguridad, los Estados miembros pueden cooperar con terceros países y emprender actividades que se consideren adecuadas a tal fin, incluidos los acuerdos de intercambios de información sobre ciberamenazas, incidentes, vulnerabilidades, herramientas y métodos, tácticas, técnicas y procedimientos, preparación y ejercicios para la gestión de crisis de ciberseguridad, formación, refuerzo de la confianza y acuerdos estructurados de intercambio de información.

(75) Deben introducirse revisiones interpares para ayudar a aprender de las experiencias compartidas, reforzar la confianza mutua y lograr un elevado nivel común de ciberseguridad. Las revisiones interpares pueden dar lugar a valiosas apreciaciones y recomendaciones que refuercen las capacidades generales de ciberseguridad, creando otra vía funcional para el intercambio de mejores prácticas entre los Estados miembros y contribuyendo a mejorar los niveles de madurez de los Estados miembros en materia de ciberseguridad. Asimismo, las revisiones interpares deben tener en cuenta los resultados de instrumentos similares, como el sistema de revisión interpares de la red de CSIRT, añadir valor y evitar duplicaciones. La aplicación de revisiones interpares se debe entender sin perjuicio de la legislación de la Unión o nacional relativa a la protección de información confidencial o clasificada.

(76) El Grupo de Cooperación debe establecer una metodología de autoevaluación para los Estados miembros, destinada a abarcar factores como el nivel de aplicación de las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación, el nivel de capacidades y la eficacia del ejercicio de los cometidos de las autoridades competentes, las capacidades operativas de los CSIRT, el nivel de aplicación de la asistencia mutua, el nivel de aplicación de los mecanismos de intercambio de información sobre ciberseguridad o cuestiones específicas de carácter transfronterizo o intersectorial. Debe alentarse a los Estados miembros a realizar autoevaluaciones de forma periódica, y a presentar y debatir los resultados de su autoevaluación en el Grupo de Cooperación.

([17]) Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, relativa a un Mecanismo de Protección Civil de la Unión (DO L 347 de 20.12.2013, p. 924).

(77) La responsabilidad de velar por la seguridad de los sistemas de redes y de información recae en gran medida en las entidades esenciales e importantes. Debe fomentarse y desarrollarse una cultura de gestión de riesgos que abarque evaluaciones del riesgo y la aplicación de medidas para la gestión de riesgos de ciberseguridad que se adecuen a los riesgos existentes.

(78) Las medidas para la gestión de riesgos de ciberseguridad deben tener en cuenta el grado de dependencia de la entidad esencial o importante de los sistemas de redes y de información, y entre ellas deben figurar medidas cuya finalidad sea la identificación de los riesgos de incidentes, así como la prevención, la detección, la respuesta y la recuperación en relación con los incidentes, así como la reducción de sus repercusiones. La seguridad de los sistemas de redes y de información debe comprender la seguridad de los datos almacenados, transmitidos y tratados. Las medidas para la gestión de riesgos de ciberseguridad deben prever un análisis sistémico que tenga en cuenta el factor humano a fin de obtener una visión completa de la seguridad del sistema de redes y de información.

(79) Dado que las amenazas para la seguridad de los sistemas de redes y de información pueden originarse por diferentes causas, las medidas para la gestión de riesgos de ciberseguridad deben basarse en un planteamiento que abarque todos los riesgos y tenga por objetivo proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a cualquier tipo de suceso, como robos, incendios, inundaciones, fallos en las telecomunicaciones o de suministro de electricidad, acceso físico no autorizado o daños a la información que posee la entidad esencial o importante y las instalaciones de procesamiento de información de la entidad, o frente a cualquier tipo de interferencia con dicha información e instalaciones, que puedan poner en peligro la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos. Por tanto, las medidas para la gestión de riesgos de ciberseguridad también deben abordar la seguridad física y del entorno de los sistemas de redes y de información, mediante la introducción de medidas para proteger dichos sistemas de redes y de información frente a fallos del sistema, errores humanos, actos malintencionados o fenómenos naturales, de conformidad con las normas europeas o internacionales, como las que figuran en la serie ISO/IEC 27000. A este respecto, las entidades esenciales e importantes deben abordar asimismo, en el marco de sus medidas para la 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 compatibles con la Directiva (UE) 2022/2557

(80) Con el fin de demostrar el cumplimiento de las medidas para la gestión de riesgos de ciberseguridad y en ausencia de esquemas europeos de certificación de la ciberseguridad adecuados que se hayan adoptado de conformidad con el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([18]), los Estados miembros, consultando al Grupo de Cooperación y al Grupo Europeo de Certificación de la Ciberseguridad, deben promover el uso de las normas europeas e internacionales pertinentes por parte de las entidades esenciales e importantes, o pueden exigir a las entidades que utilicen productos, servicios y procesos de TIC certificados.

(81) Para evitar imponer una carga financiera y administrativa desproporcionada a las entidades esenciales e importantes, las medidas para la gestión de riesgos de ciberseguridad han de ser proporcionadas en relación con los riesgos que presenta el sistema de redes y de información de que se trate, teniendo en cuenta el grado de progreso de dichas medidas y, en su caso, las normas europeas e internacionales aplicables, así como el coste de su aplicación.

(82) Las medidas para la gestión de riesgos de ciberseguridad deben ser proporcionales al grado de exposición de la entidad esencial o importante a los riesgos y al impacto social y económico que tendría un incidente. Al establecer medidas para la gestión de riesgos de ciberseguridad adaptadas a las entidades esenciales e importantes, han de tenerse debidamente en cuenta las diferencias en la exposición al riesgo de las entidades esenciales e importantes, como el carácter crítico de la entidad, los riesgos, incluidos los riesgos sociales, a los que está expuesta, el tamaño de la entidad, y la probabilidad de que se produzcan incidentes y su gravedad, incluidas sus repercusiones sociales y económicas.

([18]) 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).

(83) Las entidades esenciales e importantes deben garantizar la seguridad de los sistemas de redes y de información que utilizan en sus actividades. Esos sistemas están constituidos fundamentalmente por sistemas de redes y de información privados que son gestionados por el personal informático interno de las entidades esenciales e importantes o cuya seguridad se ha externalizado. Las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación establecidas en la presente Directiva deben aplicarse a las entidades esenciales e importantes pertinentes, independientemente de si mantienen ellas mismas sus sistemas de redes y de información o externalizan su mantenimiento.

(84) Teniendo en cuenta su naturaleza transfronteriza, los proveedores de servicios de DNS, los registros 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 de seguridad gestionados, los proveedores de mercados en línea, de motores de búsqueda en línea, y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza deben estar sujetos a un nivel elevado de armonización a nivel de la Unión. Por tanto, la aplicación de medidas para la gestión de riesgos de ciberseguridad en lo que respecta a dichas entidades debe facilitarse por medio de un acto de ejecución.

(85) Hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad y su relación con sus proveedores, como los proveedores de servicios de almacenamiento y tratamiento de datos o los proveedores de servicios de seguridad gestionados y editores de software, resulta especialmente importante habida cuenta de la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y en que agentes malintencionados han podido comprometer la seguridad de los sistemas de redes y de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Por ello, las entidades esenciales e importantes deben evaluar y tener en cuenta la calidad general y la resiliencia de los productos y los servicios, las medidas para la gestión de riesgos de ciberseguridad integradas en ellos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro. En particular, debe fomentarse que las entidades esenciales e importantes incorporen medidas para la gestión de riesgos de ciberseguridad en los acuerdos contractuales con sus proveedores y prestadores de servicios directos. Dichas entidades podrían tomar en consideración los riesgos provenientes de otros niveles de proveedores y prestadores de servicios.

(86) Entre los proveedores de servicios, los proveedores de servicios de seguridad gestionados en ámbitos como la respuesta a incidentes, las pruebas de penetración, las auditorías de seguridad y la consultoría desempeñan un papel especialmente importante prestando asistencia a las entidades en sus esfuerzos de prevención, detección, respuesta y recuperación en relación con los incidentes. No obstante, los propios proveedores de servicios de seguridad gestionados también han sido víctimas de ciberataques y plantean un riesgo especial como consecuencia de su estrecha integración en las actividades de las entidades. En consecuencia, las entidades esenciales e importantes deben redoblar su diligencia a la hora de seleccionar un proveedor de servicios de seguridad gestionados.

(87) Las autoridades competentes, en el contexto de sus funciones de supervisión, también pueden servirse de los servicios de ciberseguridad, como las auditorías de seguridad y las pruebas de penetración o la respuesta a incidentes.

(88) Las entidades esenciales e importantes deben abordar los riesgos derivados de sus interacciones y relaciones con otras partes interesadas dentro de un ecosistema más amplio, por ejemplo para luchar contra el espionaje industrial y proteger los secretos comerciales. En concreto, dichas 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 esenciales e importantes, estas deben adoptar todas las medidas para la gestión de riesgos de ciberseguridad apropiadas cuando recurran a servicios de transformación de datos y análisis de datos de terceros.

(89) Las entidades esenciales e importantes deben adoptar una gran variedad de prácticas básicas de ciberhigiene, como los principios de confianza cero, las actualizaciones de software, la configuración de dispositivos, la segmentación de la red, la gestión de la identidad y el acceso o la concienciación de los usuarios, y han de organizar formaciones para su personal y sensibilizar sobre las ciberamenazas. la captación ilegítima de datos confidenciales o las técnicas de ingeniería social. Por otra parte, dichas entidades deben evaluar sus propias capacidades de ciberseguridad y, en su caso, velar por la integración de las tecnologías de mejora de la ciberseguridad, como la inteligencia artificial o los sistemas de aprendizaje automático para reforzar sus capacidades y la seguridad de los sistemas de redes y de información.

(90) Para abordar en mayor profundidad los principales riesgos de las cadenas de suministro y ayudar a las entidades esenciales e importantes que operan en los sectores incluidos en el ámbito de aplicación de la presente Directiva a gestionar adecuadamente los riesgos relacionados con las cadenas de suministro y los proveedores, el Grupo de Cooperación, en colaboración con la Comisión y la ENISA, y, en su caso, previa consulta a las partes interesadas pertinentes, incluidas las pertenecientes a la industria, debe llevar a cabo evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas, como ya se hizo en el caso de las redes 5G a raíz de la Recomendación (UE) 2019/534 de la Comisión ([19]), con el objetivo de identificar en cada sector los servicios, sistemas o productos de TIC críticos, las correspondientes amenazas y las vulnerabilidades. Esas evaluaciones coordinadas de los riesgos de seguridad deben determinar las medidas, los planes de mitigación y las mejores prácticas frente a dependencias críticas, posibles puntos únicos de fallo, amenazas, vulnerabilidades y otros riesgos relacionados con la cadena de suministro, y deben explorar formas de fomentar en mayor medida su adopción por parte de las entidades esenciales e importantes. Entre los posibles factores de riesgo no técnicos, como la influencia indebida de un tercer país en los proveedores y prestadores de servicios, en particular en el caso de modelos de gobernanza alternativos, figuran las vulnerabilidades ocultas o las puertas traseras y posibles perturbaciones sistémicas del suministro, especialmente en caso de bloqueo tecnológico o dependencia de proveedores.

(91) Las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas, 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 de la UE de la ciberseguridad 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 coordinada de riesgos, 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 a lo largo de su ciclo de vida frente a las perturbaciones; y v) en el caso de los servicios, sistemas o productos de TIC emergentes, la importancia que puedan tener en el futuro para las actividades de las entidades. Además, debe prestarse especial atención a los servicios, sistemas o productos de TIC que proceden de terceros países y están sujetos a requisitos específicos.

(92) Con vistas a racionalizar las obligaciones 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 en relación con la seguridad de sus sistemas de redes y de información, así como para que dichas entidades y las autoridades competentes con arreglo a la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo ([20]) y al Reglamento (UE) n.º 910/2014 respectivamente puedan beneficiarse del marco jurídico establecido por la presente Directiva, incluida la designación de un CSIRT responsable de la gestión de incidentes y la participación de las autoridades competentes en cuestión en las actividades del Grupo de Cooperación y la red de CSIRT, procede incluir a dichas entidades en el ámbito de aplicación de la presente Directiva. Por consiguiente, es preciso suprimir las disposiciones correspondientes establecidas en el Reglamento (UE) n.º 910/2014 y en la Directiva (UE) 2018/1972 relativas a la imposición de requisitos de seguridad y notificación a esos tipos de entidades. Las normas sobre las obligaciones de notificación establecidas en la presente Directiva deben entenderse sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679 y en la Directiva 2002/58/CE.

(93) Las obligaciones en materia de ciberseguridad 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. Debe exigirse a los prestadores de servicios de confianza que tomen todas las medidas oportunas y proporcionadas para gestionar los riesgos a que están expuestos sus servicios, también en lo relativo a los clientes y terceros usuarios, y que notifiquen los incidentes con arreglo a la presente Directiva. Esas obligaciones en materia de ciberseguridad y notificación también deben referirse a la protección física de los servicios prestados. Los requisitos aplicables a los prestadores cualificados de servicios de confianza establecidos en el artículo 24 del Reglamento (UE) n.º 910/2014 siguen siendo de aplicación.

([19]) 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).

([20]) 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)

(94) Los Estados miembros pueden asignar a los organismos de supervisión con arreglo al Reglamento (UE) n.º 910/2014 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 de dicho Reglamento. En tal caso, las autoridades competentes con arreglo a la presente Directiva deben cooperar estrechamente y en un plazo adecuado con dichos organismos de supervisión intercambiando información pertinente para garantizar la supervisión efectiva y el cumplimiento, por parte de los prestadores de servicios de confianza, de los requisitos establecidos en la presente Directiva y en el Reglamento (UE) n.º 910/2014. En su caso, el CSIRT o la autoridad competente con arreglo a la presente Directiva debe informar inmediatamente al organismo de supervisión a efectos del Reglamento (UE) n.º 910/2014 sobre las ciberamenazas o incidentes significativos que afecten a los servicios de confianza, así como sobre los incumplimientos de la presente Directiva por parte de los prestadores de servicios de confianza. En lo que se refiere a la notificación, los Estados miembros pueden utilizar, en su caso, un punto de entrada único establecido para garantizar una notificación de incidentes común y automática tanto al organismo de supervisión con arreglo al Reglamento (UE) n.º 910/2014 como al CSIRT o la autoridad competente con arreglo a la presente Directiva.

(95) 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 ser tenidas en cuenta en la transposición de la presente Directiva, para así aprovechar los conocimientos y capacidades ya adquiridos en el marco de la Directiva (UE) 2018/1972 en lo relativo a las medidas de seguridad y las notificaciones de incidentes. La ENISA también puede elaborar orientaciones sobre requisitos de seguridad y obligaciones de 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 con arreglo a la Directiva (UE) 2018/1972, a fin de garantizar la continuación de las prácticas actuales y aprovechar los conocimientos y la experiencia adquiridos gracias a la aplicación de dicha Directiva.

(96) Dada la importancia que están adquiriendo los servicios de comunicaciones interpersonales independientes de la numeración, tal como los define la Directiva (UE) 2018/1972, es preciso garantizar que estos servicios también estén sujetos a requisitos de seguridad apropiados en vista de su naturaleza específica e importancia económica. A medida que la superficie de ataque sigue aumentando, los servicios de comunicaciones interpersonales independientes de la numeración, como los servicios de mensajería, se están convirtiendo en vectores habituales de los ataques. Los malhechores utilizan plataformas para comunicarse y atraer a las víctimas para que abran páginas web peligrosas, aumentando así la probabilidad de que se produzcan incidentes que conlleven la explotación de datos personales y, por extensión, afecten a la seguridad de los sistemas de redes y de información. Los proveedores de servicios de comunicaciones interpersonales independientes de la numeración deben garantizar un nivel de seguridad de los sistemas de redes y 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 aspectos puede considerarse que el grado de riesgo al que están expuestos estos servicios es inferior al de los servicios de comunicaciones electrónicas tradicionales. Lo mismo puede decirse de los servicios de comunicaciones interpersonales tal como se definen en la Directiva (UE) 2018/1972 que utilizan números y que no ejercen un control real sobre la transmisión de las señales.

(97) 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 de las entidades esenciales e importantes se desarrolle sin problemas, es importante que todos los proveedores de redes públicas de comunicaciones electrónicas cuenten con medidas de gestión de los riesgos de ciberseguridad apropiadas y notifiquen los incidentes significativos en este ámbito. Los Estados miembros deben velar por que se mantenga la seguridad de las redes públicas de comunicaciones electrónicas y por que se protejan sus intereses vitales en materia de seguridad frente al sabotaje y el espionaje. Dado que la conectividad internacional mejora y acelera la digitalización competitiva de la Unión y de su economía, los incidentes que afectan a los cables submarinos de comunicaciones deben notificarse al CSIRT o, en su caso, a la autoridad competente. La estrategia nacional de ciberseguridad debe tener en cuenta, en su caso, la ciberseguridad de los cables de comunicaciones submarinos e incluir una traza de los posibles riesgos de ciberseguridad y medidas paliativas para garantizar el máximo nivel de protección.

(98) A fin de salvaguardar la seguridad de las redes públicas de comunicaciones electrónicas y de los servicios de comunicaciones electrónicas disponibles al público, debe promoverse el uso de tecnologías de cifrado, y en particular el cifrado de extremo a extremo, así como conceptos de seguridad centrados en los datos, como la cartografía de datos, la segmentación, el etiquetado, las políticas y la gestión de acceso, y las decisiones de acceso automatizadas. En caso necesario, el uso del cifrado, en particular el cifrado de extremo a extremo, debe ser obligatorio para los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público de conformidad con los principios de seguridad y privacidad por defecto y desde el diseño a efectos de la presente Directiva. El uso de cifrado de extremo a extremo debe conciliarse con las facultades de los Estados miembros para garantizar la protección de sus intereses de seguridad esenciales y la seguridad pública, y para permitir la prevención, investigación, detección y enjuiciamiento de infracciones penales de conformidad con el Derecho de la Unión. Sin embargo, esto no debe debilitar el cifrado de extremo a extremo, que es una tecnología crítica para la protección eficaz de los datos y la privacidad, y para la seguridad de las comunicaciones.

(99) Para salvaguardar la seguridad y evitar los abusos y la manipulación de las redes públicas de comunicaciones electrónicas y de los servicios de comunicaciones electrónicas disponibles al público, debe promoverse el uso de normas de enrutamiento seguras con el fin de garantizar la integridad y la solidez de las funciones de enrutamiento en todo el ecosistema de proveedores de servicios de acceso a internet.

(100) Para salvaguardar la funcionalidad y la integridad de internet y fomentar la seguridad y la resiliencia del DNS, debe alentarse a las partes interesadas, incluidas las entidades del sector privado de la Unión, los proveedores de servicios de comunicaciones electrónicas disponibles al público, en particular los proveedores de servicios de acceso a internet, y los proveedores de motores de búsqueda en línea, a adoptar una estrategia de diversificación de la resolución de DNS. Además, los Estados miembros deben promover el desarrollo y la utilización de un servicio de resolución de DNS europeo público y seguro.

(101) La presente Directiva establece un enfoque en varias etapas respecto a la notificación de incidentes significativos a fin de alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a reducir la posible propagación de incidentes significativos y permita a las entidades esenciales e importantes buscar asistencia, y, por el otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente y mejore con el tiempo la ciberresiliencia de las entidades individualmente y de sectores completos. En este sentido, la presente Directiva debe incluir la notificación de incidentes que, según una evaluación inicial realizada por la entidad afectada podrían provocar perturbaciones operativas o perjuicios económicos graves para dicha entidad o podrían afectar a otras personas físicas o jurídicas causándoles perjuicios materiales o inmateriales considerables. Tal evaluación inicial debe tener en cuenta, entre otros aspectos, los sistemas de redes y de información afectados, y en particular su importancia para la prestación de los servicios de la entidad, la gravedad y las características técnicas de la ciberamenaza, así como las vulnerabilidades subyacentes que se estén aprovechando y la experiencia de la entidad con incidentes similares. Indicadores como la medida en que se ve afectado el funcionamiento del servicio, la duración de un incidente o el número de destinatarios de los servicios afectados podrían ser importantes a la hora de determinar si la perturbación operativa del servicio es grave.

(102) Cuando las entidades esenciales o importantes tengan conocimiento de un incidente significativo, deben estar obligadas a presentar una alerta temprana sin demora indebida y, en cualquier caso, en el plazo de veinticuatro horas. Dicha alerta temprana debe ir seguida de una notificación del incidente. Las entidades afectadas deben presentar una notificación del incidente sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas a partir del momento en que tengan conocimiento del incidente significativo, con el objetivo, en particular, de actualizar la información presentada mediante la alerta temprana y exponer una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles. Se ha de presentar un informe final a más tardar un mes después de la notificación del incidente. La alerta temprana solo debe incluir la información necesaria para que el CSIRT, o, en su caso, la autoridad competente, tenga constancia del incidente significativo y la entidad afectada pueda solicitar asistencia, en caso de que sea necesario. En su caso, dicha alerta temprana debe indicar si se sospecha que el incidente significativo está causado por actos ilícitos o malintencionados y si es probable que tenga repercusiones transfronterizas. Los Estados miembros deben velar por que la obligación de presentar dicha alerta temprana, o la posterior notificación del incidente, no detraiga los recursos de la entidad notificante de las actividades relacionadas con la gestión del incidente, que deben ser prioritarias, a fin de evitar que las obligaciones de notificación de incidentes desvíen recursos de la gestión de la

respuesta a incidentes significativos o comprometan de otro modo los esfuerzos de las entidades a este respecto. En el caso de que el incidente siga en curso en el momento de la presentación del informe final, los Estados miembros deben velar por que las entidades afectadas presenten un informe de situación en ese momento y un informe final en el plazo de un mes a partir de que hayan gestionado el incidente significativo.

(103) Cuando proceda, las entidades esenciales e importantes deben informar sin demora a los destinatarios de sus servicios de las medidas o soluciones que pueden aplicar para reducir el riesgo resultante de una ciberamenaza significativa. En su caso, y en particular cuando sea probable que se materialice la ciberamenaza significativa, dichas entidades también deben informar a los destinatarios de sus servicios de la propia amenaza. La exigencia de informar de tales amenazas a los destinatarios debe cumplirse en la medida de lo posible, pero no exime a dichas entidades de la obligación de tomar a sus expensas medidas inmediatas y adecuadas e inmediatas para prevenir o subsanar cualquier ciberamenaza y restablecer el nivel normal de seguridad del servicio. La mencionada información sobre las ciberamenazas significativas a los destinatarios del servicio debe facilitarse de forma gratuita y la información debe estar redactada en un lenguaje fácil de comprender.

(104) Los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público deben aplicar la seguridad desde el diseño y por defecto, e informar a los destinatarios de los servicios sobre ciberamenazas significativas y sobre las medidas que pueden adoptar para proteger la seguridad de sus dispositivos y comunicaciones, por ejemplo, utilizar determinados tipos de software o tecnologías de cifrado.

(105) Adoptar un planteamiento proactivo ante las ciberamenazas es un elemento vital en la gestión de los riesgos de ciberseguridad que debería permitir a las autoridades competentes prevenir eficazmente que las ciberamenazas se materialicen en incidentes que puedan ocasionar perjuicios materiales o inmateriales considerables. La notificación de ciberamenazas es de crucial importancia a este respecto. A tal fin, se alienta a las entidades a que informen voluntariamente de las ciberamenazas.

(106) A fin de simplificar la notificación de la información exigida con arreglo a la presente Directiva, así como de reducir la carga administrativa para las entidades, los Estados miembros deben ofrecer medios técnicos como un punto de entrada único, sistemas automatizados, formularios en línea, interfaces de fácil uso, modelos, plataformas específicas para el uso de entidades, con independencia de que estén incluidas en el ámbito de aplicación de la presente Directiva, para la presentación de la información pertinente que ha de notificarse. La financiación de la Unión para apoyar la aplicación de la presente Directiva, en particular en el marco del programa Europa Digital establecido por el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo ([21]), podría incluir el apoyo a los puntos de entrada únicos. Además, las entidades se ven con frecuencia en la situación de que un incidente concreto, por sus características, debe notificarse a varias autoridades para cumplir las obligaciones de notificación recogidas en distintos instrumentos jurídicos. Estos casos crean cargas suplementarias y también pueden generar inseguridad en cuanto al formato y el procedimiento de tales notificaciones. Cuando se establezca un punto de entrada único, se alienta a los Estados miembros a que también utilicen dicho punto de entrada único para las notificaciones de incidentes de seguridad exigidas por otros actos legislativos de la Unión, como el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. El uso de dicho punto de entrada único para la notificación de incidentes de seguridad con arreglo al Reglamento (UE) 2016/679 y a la Directiva 2002/58/CE no debe afectar a la aplicación de las disposiciones del Reglamento (UE) 2016/679 y de la Directiva 2002/58/CE, en particular las relativas a la independencia de las autoridades a que estos actos se refieren. La ENISA, en colaboración con el Grupo de Cooperación, debe elaborar modelos de notificación comunes mediante directrices que simplifiquen y racionalicen la información que ha de notificarse con arreglo al Derecho de la Unión y reduzcan la carga administrativa de las entidades notificantes.

(107) Cuando se sospeche que un incidente guarda relación con actividades delictivas graves con arreglo al Derecho de la Unión o nacional, los Estados miembros deben alentar a las entidades esenciales e importantes, sobre la base de las normas procesales penales aplicables con arreglo al Derecho de la Unión, a denunciar ante las autoridades pertinentes encargadas de hacer cumplir la ley los incidentes que presuntamente sean de naturaleza delictiva grave. Cuando proceda, y sin perjuicio de las normas de protección de datos personales aplicables a Europol, conviene que el Centro Europeo de Ciberdelincuencia (EC3) y la ENISA faciliten la coordinación entre las autoridades competentes y las autoridades encargadas de hacer cumplir la ley de los distintos Estados miembros.

([21]) Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 (DO L 166 de 11.5.2021, p. 1).

(108) 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 a que se refieren el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE.

(109) Mantener bases de datos precisas y completas con los datos de registro de los nombres de dominio (los denominados «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 toda la Unión. A tal fin específico, los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben estar obligados a tratar determinados datos necesarios para alcanzar dicho objetivo. Dicho tratamiento debe constituir una obligación legal en el sentido del artículo 6, apartado 1, letra c), del Reglamento (UE) 2016/679. Dicha obligación se entenderá sin perjuicio de la posibilidad de recopilar datos de registro de nombres de dominio para otros fines, por ejemplo sobre la base de acuerdos contractuales o requisitos legales establecidos en otro Derecho de la Unión o nacional. Tal obligación tiene por objeto lograr un conjunto completo y preciso de datos de registro y no debe dar lugar a la recopilación de los mismos datos en múltiples ocasiones. Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben cooperar entre sí para evitar la duplicación de esa tarea.

(110) La disponibilidad y la accesibilidad oportuna de los datos de registro de nombres de dominio para los solicitantes de acceso legítimos son esenciales para prevenir y combatir los abusos del DNS, así como para prevenir y detectar incidentes y responder ante ellos. Se ha de entender por solicitante de acceso legítimo toda persona física o jurídica que presente una solicitud en virtud del Derecho de la Unión o nacional. Pueden incluir a las autoridades competentes con arreglo a la presente Directiva y aquellas autoridades competentes con arreglo al Derecho de la Unión o nacional para la prevención, la investigación o el enjuiciamiento de infracciones penales y los CERT o los CSIRT. Los registros de nombre dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio también deben permitir el acceso lícito a datos específicos sobre el registro de nombres de dominio necesarios para los fines de la solicitud de acceso por parte de solicitantes de acceso legítimos, de conformidad con el Derecho de la Unión en materia de protección de datos. La solicitud de los solicitantes de acceso legítimo debe ir acompañada de una exposición de motivos que permita evaluar la necesidad de acceder a los datos.

(111) Al objeto de garantizar la disponibilidad de datos precisos y completos sobre el registro de nombres de dominio, los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben recabar y garantizar la integridad y disponibilidad de los datos de registro de nombres de dominio. Concretamente, los registros de nombres de dominio de primer nivel y las entidades que presten servicios de registro de nombres de dominio 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, de conformidad con el Derecho de la Unión en materia de protección de datos. Dichas políticas y procedimientos deben tener en cuenta, en la medida de lo posible, las normas elaboradas por las estructuras de gobernanza multilateral a nivel internacional. Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben adoptar y aplicar procedimientos proporcionados para verificar los datos de registro de nombres de dominio. Dichos procedimientos deben reflejar las mejores prácticas del sector y, en la medida de lo posible, los progresos realizados en el ámbito de la identificación electrónica. Cabe señalar como ejemplos de procedimientos de verificación los controles a priori realizados en el momento del registro y los controles a posteriori realizados después del registro. Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben verificar como mínimo uno de los medios de contacto del solicitante de registro.

(112) Los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben estar obligados a poner a disposición del público los datos de registro de nombres de dominio que quedan fuera del ámbito de aplicación del Derecho de la Unión en materia de protección de datos, como por ejemplo los datos referentes a personas jurídicas, en consonancia con el preámbulo del Reglamento (UE) 2016/679. En el caso de las personas jurídicas, los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio deben poner a disposición del público como mínimo el nombre del solicitante de registro y el número de teléfono de contacto. También debe publicarse la dirección de correo electrónico de contacto, siempre que no contenga datos personales, como es el caso del uso de alias de correo electrónico o cuentas funcionales o sistemas similares. Los registros de nombres de dominio de primer nivel y las entidades que presten servicios de registro de nombres de dominio 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 exigir a los registros de nombres de dominios de primer nivel y a las entidades que prestan servicios de registro de nombres de dominio que respondan sin demora indebida a las solicitudes de divulgación de datos de registro de nombres de dominio provenientes de solicitantes de acceso legítimos. Los registros de nombres de dominio de

primer nivel y las entidades que prestan servicios de registro de nombres de dominio 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. Dichas políticas y procedimientos deben tener en cuenta, en la medida de lo posible, las directrices y las normas elaboradas por las estructuras de gobernanza multilateral a nivel internacional. El procedimiento de acceso también podría incluir el uso de una interfaz, un portal u otra herramienta técnicas que proporcionen un sistema eficiente para la solicitud de datos de registro y el acceso a ellos. Con vistas a promover prácticas armonizadas en todo el mercado interior, la Comisión, sin perjuicio de las competencias del Comité Europeo de Protección de Datos, puede proporcionar directrices sobre dichos procedimientos que tengan en cuenta, en la medida de lo posible, las normas elaboradas por las estructuras de gobernanza multilateral a nivel internacional. Los Estados miembros deben garantizar que todos los tipos de acceso a los datos personales y no personales de registro de nombres de dominio sean gratuitos.

(113) Las entidades comprendidas en el ámbito de aplicación de la presente Directiva deben considerarse sometidas a la jurisdicción del Estado miembro en el que están establecidas. No obstante, los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público deben considerarse sometidos a la jurisdicción del Estado miembro en el que prestan sus servicios. Los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales deben considerarse sometidos a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal en la Unión. Las entidades de la Administración pública deben estar sometidas a la jurisdicción del Estado miembro que las haya establecido. Si la entidad presta servicios o está establecida en más de un Estado miembro, debe estar sometida a la jurisdicción separada y concurrente de cada uno de ellos. Las autoridades competentes de esos Estados miembros deben cooperar, prestarse asistencia mutua y, cuando proceda, emprender medidas conjuntas de supervisión. Cuando los Estados miembros ejerzan su competencia, no deben imponer medidas de ejecución ni sanciones más de una vez por una misma conducta, en consonancia con el principio *ne bis in idem*.

(114) 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, las entidades que presten servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales solo un Estado miembro debe tener jurisdicción sobre esas entidades. La jurisdicción debe atribuirse al Estado miembro en el que se encuentre el establecimiento principal en la Unión de la entidad de que se trate. 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 los sistemas de redes y 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. Se debe considerar que el establecimiento principal está en el Estado miembro 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 entidades en la Unión. Si no puede determinarse dicho Estado miembro o si dichas decisiones no se toman en la Unión, debe considerarse que el establecimiento principal se encuentra en el Estado miembro en el que se llevan a cabo las operaciones de ciberseguridad. Si no puede determinarse dicho Estado miembro, 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.

(115) Si un proveedor de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público presta un servicio de DNS recursivo disponible al público solamente como parte del servicio de acceso a internet, la entidad debe considerarse comprendida en el ámbito de competencia de todos los Estados miembros en los que presta sus servicios.

(116) En situaciones en las que los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales no estén establecidos en la Unión pero ofrezcan servicios dentro de ella, deben designar un representante en la Unión. Para determinar si dicha entidad ofrece servicios en la Unión, debe determinarse si 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, debe considerarse insuficiente 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 lengua, o la mención de clientes o usuarios que estén en la Unión, podría 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 dirigirse al representante. 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 que establece la presente Directiva, también por lo que respecta a la notificación de incidentes.

(117) A fin de garantizar una visión clara de los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales que presten servicios en toda la Unión y estén comprendidos en el ámbito de aplicación de la presente Directiva, la ENISA debe crear y mantener un registro de estas entidades, basado en la información recibida de los Estados miembros, si procede mediante los mecanismos nacionales establecidos para que las entidades se registren ellas mismas. Los puntos de contacto únicos deben transmitir a la ENISA la información y cualquier modificación de la misma. Con objeto de asegurar la exactitud y exhaustividad de la información que se ha de incluir en el registro, los Estados miembros pueden presentar a la ENISA la información disponible en cualquier registro nacional sobre esas 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. La ENISA debe establecer protocolos adecuados de clasificación y gestión de la información con objeto de garantizar la seguridad y confidencialidad de la información divulgada, y ha de restringir el acceso, el almacenamiento y la transmisión de dicha información a los usuarios previstos.

(118) Cuando se intercambie, notifique o comparta de cualquiera forma con arreglo a las disposiciones de la presente Directiva información que esté clasificada de conformidad con el Derecho de la Unión o nacional deben aplicarse las correspondientes normas específicas sobre el tratamiento de información clasificada. Además, la ENISA debe contar con la infraestructura, los procedimientos y las normas necesarios para tratar información sensible y clasificada de conformidad con las normas de seguridad aplicables para proteger la información clasificada de la Unión.

(119) Puesto que las ciberamenazas son cada vez más complejas y sofisticadas, el éxito de las medidas de detección de tales amenazas y su 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 tales amenazas se materialicen en incidentes 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.

(120) Debe animarse a las entidades para que, con la asistencia de los Estados miembros, aprovechen colectivamente sus conocimientos y experiencias prácticas individuales a nivel estratégico, táctico y operativo para reforzar sus capacidades de prevención, detección, respuesta y recuperación ante incidentes y mitigación de su impacto. Por consiguiente, es necesario propiciar la creación a nivel de la Unión de acuerdos voluntarios de intercambio de información sobre ciberseguridad. Para ello, los Estados miembros también deben asistir y alentar activamente a las entidades, como las dedicadas a los servicios y la investigación en el ámbito de la ciberseguridad, así como a las entidades pertinentes que no quedan comprendidas en el ámbito de aplicación de la presente Directiva, para que participen en tales mecanismos de intercambio de información sobre ciberseguridad. Dichos mecanismos deben establecerse de conformidad con las normas de competencia de la Unión y el Derecho de la Unión en materia de protección de datos.

(121) El tratamiento de datos personales, en la medida en que sea necesario y proporcionado para garantizar la seguridad de los sistemas de redes y de información por parte de las entidades esenciales e importantes, podría considerarse lícito sobre la base de que dicho tratamiento cumple una obligación jurídica a la que está sujeto el responsable del tratamiento, de conformidad con los requisitos del artículo 6, apartado 1, letra c), y del artículo 6, apartado 3, del Reglamento (UE) 2016/679. El tratamiento de datos personales también podría ser necesario para la satisfacción de intereses legítimos perseguidos por entidades esenciales e importantes, así como por proveedores de tecnologías y servicios de seguridad que actúen en nombre de dichas entidades, de conformidad con el artículo 6, apartado 1, letra f), del Reglamento (UE) 2016/679, incluso cuando dicho tratamiento sea necesario para los mecanismos de intercambio de información sobre ciberseguridad o la notificación voluntaria de información pertinente de conformidad con la presente Directiva. Las medidas relacionadas con la prevención, la detección, la identificación, la contención y el análisis de incidentes y la respuesta ante estos, las 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, 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 pueden requerir el tratamiento de determinadas categorías de datos personales, como direcciones IP, localizadores uniformes de recursos (URL), nombres de dominio, direcciones de correo electrónico y, si revelan datos personales, sellos de tiempo. El tratamiento de datos personales por parte de las autoridades competentes, los puntos de contacto únicos y los CSIRT podría constituir una obligación legal o considerarse necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento de los datos de conformidad con el artículo 6, apartado 1, letras c) o e), y el artículo 6, apartado 3, del Reglamento (UE) 2016/679, o para perseguir un interés legítimo de entidades esenciales e importantes a que se refiere el artículo 6, apartado 1, letra f), de dicho Reglamento. Además, el Derecho nacional podría establecer normas que permitan a las autoridades competentes, los puntos de contacto únicos y los CSIRT, en la medida en que sea necesario y proporcionado a efectos de garantizar la seguridad de los sistemas de redes y de información de las entidades esenciales e importantes, tratar categorías especiales de datos personales de conformidad con el artículo 9 del Reglamento (UE) 2016/679, en particular estableciendo medidas adecuadas y específicas para salvaguardar los derechos e intereses fundamentales de las personas físicas, incluidas limitaciones técnicas a la reutilización de dichos datos y el uso de medidas de última generación en materia de seguridad y protección de la intimidad, como la seudonimización o el cifrado cuando la anonimización pueda afectar significativamente al objetivo perseguido.

(122) 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 medidas 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 que recaen sobre dichas entidades y sobre 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*. Por lo tanto, las entidades importantes no deben tener la obligación de documentar sistemáticamente la conformidad con las medidas para la gestión de riesgos de ciberseguridad, a la vez 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 se pongan en conocimiento de las autoridades competentes pruebas, indicios o información que dichas autoridades estimen que pueden sugerir un posible incumplimiento de la presente Directiva. Por ejemplo, tales 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 podría proceder de otras actividades realizadas por las autoridades competentes en el ejercicio de sus funciones.

(123) La ejecución de funciones de supervisión por parte de las autoridades competentes no debe obstaculizar innecesariamente las actividades empresariales de la entidad de que se trate. Cuando las autoridades competentes lleven a cabo sus tareas de supervisión en relación con entidades esenciales, en particular la realización de inspecciones in situ y la supervisión a distancia, la investigación de incumplimientos de la presente Directiva y la realización de auditorías de seguridad o exámenes de seguridad, deben minimizar el impacto en las actividades empresariales de la entidad de que se trate.

(124) En el ejercicio de la supervisión a priori, las autoridades competentes deben poder decidir sobre la priorización del uso 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 basándose en las metodologías de supervisión que deben aplicar un enfoque basado en el riesgo. Más concretamente, estas metodologías podrían incluir criterios o indicadores para la clasificación de las entidades esenciales en categorías de riesgo junto 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. Tales metodologías de supervisión también se podrían complementar con programas de trabajo y evaluarse y revisarse de manera periódica, en particular en aspectos tales como la dotación de recursos y las necesidades. En lo relativo a las entidades de la Administración pública, las facultades de supervisión se pueden aplicar en consonancia con los marcos legislativos e institucionales nacionales.

(125) Las autoridades competentes deben velar por que sus funciones de supervisión en relación con las entidades esenciales e importantes sean llevadas a cabo por profesionales cualificados, que deben tener las competencias necesarias para llevar a cabo dichas tareas, en particular en lo que respecta a la realización de inspecciones in situ y funciones de supervisión a distancia, como la detección de deficiencias en las bases de datos, equipos informáticos, cortafuegos, cifrado y las redes. Dichas inspecciones y dicha supervisión deben llevarse a cabo de manera objetiva.

(126) En casos debidamente justificados en los que tenga conocimiento de una ciberamenaza significativa o de un riesgo inminente, la autoridad competente debe poder adoptar decisiones de ejecución inmediatas con el fin de prevenir incidentes o responder ante ellos.

(127) A fin de garantizar el cumplimiento efectivo, debe fijarse una lista mínima de poderes de ejecución que pueden ejercerse por infracción de las medidas para la gestión de riesgos de ciberseguridad y de las obligaciones de notificación previstas en la presente Directiva, mediante el establecimiento de un marco claro y coherente para tales medidas de ejecución en toda la Unión. Debe prestarse la debida atención a la naturaleza, gravedad y duración de la infracción de la presente Directiva, los perjuicios materiales o inmateriales originados, la intencionalidad o negligencia en la infracción, las medidas adoptadas para prevenir o paliar los perjuicios materiales o inmateriales, el grado de responsabilidad o cualquier infracción anterior pertinente, el grado de cooperación con la autoridad competente y cualquier otra circunstancia agravante o atenuante. Las medidas de ejecución, incluidas las multas administrativas, deben ser proporcionadas y su imposición 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 («la Carta»), entre ellas, el derecho a la tutela judicial efectiva, a un juicio justo, la presunción de inocencia y los derechos de la defensa.

(128) La presente Directiva no exige a los Estados miembros que establezcan la responsabilidad penal o civil con respecto a las personas físicas responsables de garantizar que una entidad cumpla lo dispuesto en la presente Directiva por los perjuicios sufridos por terceros como consecuencia de un incumplimiento de la presente Directiva.

(129) 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.

(130) Si las multas administrativas se imponen a una entidad esencial o importante que sea 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, la autoridad competente debe tener en cuenta el nivel general de ingresos prevalente 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.

(131) Los Estados miembros deben poder 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 de la Unión Europea.

(132) En los casos en que la presente Directiva no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en el supuesto de infracción grave de la presente Directiva, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. El Derecho nacional debe determinar la naturaleza de dichas sanciones y si son penales o administrativas.

(133) Con vistas a reforzar más aún la eficacia y el carácter disuasorio de las medidas de ejecución aplicables por la infracción de la presente Directiva, las autoridades competentes deben estar facultadas para suspender temporalmente o solicitar la suspensión temporal de una certificación o autorización referente a una parte o la totalidad de los servicios pertinentes prestados o a las actividades realizadas por una entidad esencial y solicitar la imposición de una prohibición temporal de que una persona física ejerza funciones de dirección a nivel de director general o representante legal. Habida cuenta de su gravedad y repercusión en las actividades de las entidades y, en última instancia, en sus usuarios, dichas suspensiones o prohibiciones temporales deben aplicarse exclusivamente de manera proporcional a la gravedad de la infracción y teniendo en cuenta las circunstancias de cada caso, en particular si la infracción fue intencionada o negligente, y toda medida adoptada para prevenir o paliar los perjuicios materiales o inmateriales sufridos. Las suspensiones o prohibiciones temporales 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 solo 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 suspensiones o prohibiciones temporales. La imposición de tales suspensiones o prohibiciones temporales debe estar sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva, a un juicio justo, a la presunción de inocencia y los derechos de la defensa.

(134) A fin de garantizar que las entidades cumplan las obligaciones que les incumben con arreglo a la presente Directiva, los Estados miembros deben cooperar y prestarse asistencia mutua en relación con las medidas de supervisión y ejecución, en particular cuando una entidad preste servicios en más de un Estado miembro o cuando sus sistemas de redes y de información estén situados en un Estado miembro distinto de aquel en el que presta servicios. Cuando preste asistencia, la autoridad competente requerida debe adoptar medidas de supervisión o ejecución de conformidad con el Derecho nacional. A fin de garantizar el buen funcionamiento de la asistencia mutua en virtud de la presente Directiva, las autoridades competentes deben utilizar el Grupo de Cooperación como foro para debatir casos y solicitudes concretas de asistencia.

(135) Con el fin de asegurar la supervisión y la ejecución efectivas, en particular en una situación que presente una dimensión transfronteriza, los Estados miembros que hayan recibido una solicitud de asistencia mutua deben, dentro de los límites de dicha solicitud, tomar medidas adecuadas de supervisión y ejecución en relación con la entidad objeto de tal petición, y que presta servicios o que tiene un sistema de redes y de información en el territorio de dicho Estado miembro.

(136) 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 los incumplimientos de la presente Directiva relacionadas con los datos personales.

(137) 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 entidades esenciales e importantes. Por consiguiente, los órganos de dirección de las entidades esenciales e importantes deben aprobar las medidas de gestión de riesgos de ciberseguridad y supervisar su aplicación.

(138) A fin de garantizar un elevado nivel común de ciberseguridad en toda la Unión sobre la base de la presente Directiva, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE, por lo que respecta a complementar la presente Directiva especificando qué categorías de entidades esenciales e importantes han de estar obligadas a utilizar determinados productos de TIC, servicios de TIC y procesos de TIC certificados u obtener una certificación en el marco de un esquema europeo de certificación de la ciberseguridad. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([22]). En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

([22]) DO L 123 de 12.5.2016, p. 1.

(139) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución para establecer las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Cooperación y los requisitos técnicos, metodológicos y sectoriales relativos a las medidas para la gestión de riesgos de ciberseguridad, así como para especificar en mayor medida el tipo de información, el formato y el procedimiento de las notificaciones de incidentes, ciberamenazas y cuasiincidentes y de las comunicaciones significativas de ciberamenazas, así como los casos en que un incidente debe considerarse significativo. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([23]).

(140) La Comisión debe revisar periódicamente lo dispuesto en la presente Directiva, previa consulta a las partes interesadas, en particular para determinar si resulta conveniente proponer enmiendas a raíz de cambios en la situación social, política, de la tecnología o el mercado. Como parte de esas revisiones, la Comisión debe evaluar la importancia de la magnitud de las entidades de que se trate, y los sectores, los subsectores y los tipos de entidades a que se refieren los anexos de la presente Directiva para el funcionamiento de la economía y la sociedad por lo que respecta a la ciberseguridad. La Comisión debe evaluar, entre otros aspectos, si los proveedores, comprendidos en el ámbito de aplicación de la presente Directiva, son designados como plataformas en línea de muy gran tamaño en el sentido del artículo 33 del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo ([24]) podrían identificarse como entidades esenciales a los efectos de la presente Directiva.

(141) La presente Directiva crea nuevos cometidos para la ENISA, reforzando así su papel, y también podría dar lugar a que la ENISA tenga que desempeñar los cometidos que actualmente le atribuye el Reglamento (UE) 2019/881 con un mayor nivel de exigencia. A fin de garantizar que la ENISA disponga de los recursos financieros y humanos necesarios para llevar a cabo sus cometidos actuales y sus nuevos cometidos, así como para cumplir con un nivel de ejecución más elevado de aquellos cometidos resultantes de su papel reforzado, debe incrementarse su presupuesto en consecuencia. Además, a fin de garantizar un uso eficiente de los recursos, la ENISA debe tener mayor flexibilidad en la forma en que puede asignar recursos internamente con el propósito de desempeñar sus cometidos eficazmente y satisfacer las expectativas.

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

(143) La presente Directiva respeta los derechos fundamentales y los principios reconocidos por la Carta, 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, a un juicio justo, la presunción de inocencia y los derechos de la defensa. El derecho una tutela judicial efectiva se extiende a los destinatarios de los servicios prestados por entidades esenciales e importantes. La presente Directiva debe aplicarse con arreglo a esos derechos y principios.

(144) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 ([25]) del Parlamento Europeo y del Consejo, emitió su dictamen el 11 de marzo de 2021 ([26]).

---

([23]) 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).

([24]) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277 de 27.10.2022, p. 1).

([25]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

([26]) DO C 183 de 11.5.2021, p. 3.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

**DISPOSICIONES GENERALES**

*Artículo 1*

**Objeto**

1. La presente Directiva establece medidas que tienen por objeto alcanzar un elevado nivel común de ciberseguridad en toda la Unión con el objetivo de mejorar el funcionamiento del mercado interior.

2. A tal fin, la presente Directiva establece:

a) obligaciones que requieren que los Estados miembros adopten estrategias nacionales de ciberseguridad y designen o establezcan autoridades competentes, autoridades de gestión de crisis de ciberseguridad, puntos de contacto únicos sobre ciberseguridad (en lo sucesivo, «puntos de contacto únicos») y equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés);

b) medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades cuyo tipo se enmarca en los anexos I o II; así como para las entidades identificadas como críticas con arreglo a la Directiva (UE) 2022/2557;

c) normas y obligaciones relativas al intercambio de información sobre ciberseguridad;

d) obligaciones de supervisión y ejecución para los Estados miembros.

*Artículo 2*

**Ámbito de aplicación**

1. La presente Directiva se aplicará a las entidades públicas o privadas de alguno de los tipos mencionados en los anexos I o II que sean consideradas medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE, o que superen los límites máximos para las medianas empresas previstos en el apartado 1 de dicho artículo, y que presten sus servicios o lleven a cabo sus actividades en la Unión.

El artículo 3, apartado 4, del anexo de dicha Recomendación no se aplicará a efectos de la presente Directiva.

2. Independientemente de su tamaño, la presente Directiva también se aplicará a las entidades de alguno de los tipos mencionados en los anexos I o II cuando:

a) los servicios son prestados por:

   i) proveedores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público;

   ii) prestadores de servicios de confianza;

   iii) registros de nombres de dominio de primer nivel y proveedores de servicios de sistema de nombres de dominio;

b) la entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas;

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

d) una 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;

e) la entidad sea crítica a la luz de su importancia específica a nivel nacional o regional para el sector o tipo de servicio en concreto o para otros sectores interdependientes en el Estado miembro;

f) la entidad sea una entidad de la Administración pública:

i) central, definida por un Estado miembro de conformidad con el Derecho nacional, o

ii) regional, definida por un Estado miembro de conformidad con el Derecho nacional, que, tras una evaluación basada en el riesgo, presta servicios cuya perturbación podría tener un impacto significativo en actividades sociales o económicas críticas.

3. Independientemente de su tamaño, la presente Directiva se aplica a las entidades que se identifiquen como entidades críticas con arreglo a la Directiva (UE) 2022/2557

4. Independientemente de su tamaño, la presente Directiva se aplica a las entidades que presten servicios de registro de nombres de dominio.

5. Los Estados miembros podrán disponer que la presente Directiva se aplique a:

a) entidades de la Administración pública a nivel local;

b) centros de enseñanza, en particular cuando lleven a cabo actividades críticas de investigación.

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

7. La presente Directiva no se aplicará a las entidades de la Administración pública que lleven a cabo sus actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la garantía del cumplimiento de la ley, incluidas la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales.

8. Los Estados miembros podrán eximir a las entidades específicas que llevan a cabo actividades en los ámbitos de la defensa, la seguridad nacional, la seguridad pública o la garantía del cumplimiento de la ley, incluidas las actividades relativas a la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, o que prestan servicios exclusivamente a entidades de la Administración pública a que se refiere el apartado 7 del presente artículo, de las obligaciones establecidas en el artículo 21 o en el artículo 23 en relación con dichas actividades o servicios. En tales casos, las medidas de supervisión y garantía del cumplimiento a que se refiere el capítulo VII no se aplicarán en relación con esas actividades o servicios específicos. Cuando las entidades realicen actividades o presten servicios exclusivamente del tipo contemplado en el presente apartado, los Estados miembros podrán decidir eximir también a dichas entidades de las obligaciones establecidas en los artículos 3 y 27.

9. Los apartados 7 y 8 no se aplicarán cuando una entidad actúe como prestador de servicios de confianza.

10. La presente Directiva no se aplicará a las entidades que los Estados miembros hayan excluido del ámbito de aplicación del Reglamento (UE) 2022/2554 de conformidad con el artículo 2, apartado 4, de dicho Reglamento.

11. 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.

12. La presente Directiva se entenderá sin perjuicio del Reglamento (UE) 2016/679, la Directiva 2002/58/CE, las Directivas 2011/93/UE ([27]) y 2013/40/UE ([28]) del Parlamento Europeo y del Consejo y la Directiva (UE) 2022/2557.

13. 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 o 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 interesadas.

([27]) 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).

([28]) 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).

14. Las entidades, las autoridades competentes, los puntos de contacto únicos y los CSIRT tratarán los datos personales en la medida necesaria para los fines de la presente Directiva y de conformidad con el Reglamento (UE) 2016/679; en particular, dicho tratamiento se basará en su artículo 6.

El tratamiento de datos personales en virtud de la presente Directiva por parte de los proveedores de redes públicas de comunicaciones electrónicas o los proveedores de servicios de comunicaciones electrónicas disponibles para el público se llevará a cabo de conformidad con el Derecho de la Unión en materia de protección de datos y de la intimidad aplicables, en particular la Directiva 2002/58/CE.

*Artículo 3*

**Entidades esenciales e importantes**

1. A efectos de la presente Directiva, las siguientes entidades se considerarán entidades esenciales:

a) entidades de alguno de los tipos mencionados en el anexo I que superen los límites máximos previstos en el artículo 2, apartado 1, del anexo de la Recomendación 2003/361/CE para las medianas empresas;

b) prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel, así como proveedores de servicios de DNS, independientemente de su tamaño;

c) proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público que sean consideradas medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE;

d) entidades de la Administración pública a que se refiere el artículo 2, apartado 2, letra f) inciso i);

e) cualquier otra entidad de uno de los tipos mencionados en los anexos I o II que un Estado miembro identifique como entidad esencial en virtud del artículo 2, apartado 2, letras b) a e);

f) entidades identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557 a que se refiere el artículo 2, apartado 3, letra f), de la presente Directiva;

g) si así lo dispone el Estado miembro, las entidades identificadas por dicho Estado miembro antes del 16 de enero de 2023 como operadores de servicios esenciales de conformidad con la Directiva (UE) 2016/1148 o el Derecho nacional.

2. A efectos de la presente Directiva, se considerarán entidades importantes todas las entidades de uno de los tipos mencionados en los anexos I o II que no puedan considerarse entidades esenciales con arreglo al apartado 1 del presente artículo. Ello incluye las entidades que un Estado miembro identifique como entidades importantes en virtud del artículo 2, apartado 2, letras b) a e).

3. A más tardar el 17 de abril de 2025, los Estados miembros deben elaborar una lista de las entidades esenciales e importantes así como de las entidades que prestan servicios de registro de nombres de dominio. Posteriormente, los Estados miembros revisarán la lista con regularidad, al menos cada dos años, y si procede, la actualizarán.

4. A efectos de la elaboración de la lista a que se refiere el apartado 3, los Estados miembros requerirán a las entidades a que se refiere dicho apartado que presenten al menos la siguiente información a las autoridades competentes:

a) el nombre de la entidad;

b) la dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono;

c) si procede, el sector y el subsector pertinentes a que se refieren los anexos I o II, y

d) si procede, una lista de los Estados miembros en los que prestan servicios comprendidos en el ámbito de aplicación de la presente Directiva.

Las entidades a que se refiere el apartado 3 notificarán sin demora cualquier cambio en la información presentada en virtud del párrafo primero del presente apartado y, en cualquier caso, en el plazo de dos semanas desde la fecha en que se produjo el cambio.

La Comisión, asistida por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), deberá proporcionar sin demora indebida directrices y plantillas relativas a las obligaciones establecidas en el presente apartado.

Los Estados miembros podrán establecer mecanismos nacionales para que las entidades se registren ellas mismas.

5. A más tardar el 17 de abril de 2025, y posteriormente cada dos años, las autoridades competentes notificarán:

a) a la Comisión y al Grupo de Cooperación, el número de entidades esenciales e importantes enumeradas conforme al apartado 3 respecto de cada sector y subsector a que se refieren los anexos I o II, y

b) a la Comisión la información pertinente sobre el número de entidades esenciales e importantes identificadas en virtud del artículo 2, apartado 2, letras b) a e), el sector y subsector a que se refieren los anexos I o II a los que pertenecen, el tipo de servicio que prestan y la disposición, de entre las establecidas en el artículo 2, apartado 2, letras b) a e), en virtud de la cual fueron identificados.

6. Hasta el 17 de abril de 2025 y a petición de la Comisión, los Estados miembros podrán notificar a la Comisión los nombres de las entidades esenciales e importantes a que se refiere el apartado 5, letra b).

*Artículo 4*

**Actos jurídicos sectoriales de la Unión**

1. Cuando los actos jurídicos de carácter sectorial de la Unión requieran que las entidades esenciales o importantes adopten medidas para la gestión de riesgos de ciberseguridad o notifiquen los incidentes 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 garantía del cumplimiento recogidas en el capítulo VII. Cuando los actos jurídicos sectoriales de la Unión no cubran 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 los actos jurídicos sectoriales de la Unión en cuestión.

2. Los requisitos a que se refiere el apartado 1 del presente artículo se considerarán de efecto equivalente a las obligaciones establecidas en la presente Directiva cuando:

a) las medidas para la gestión de riesgos de ciberseguridad sean al menos equivalentes en sus efectos a las previstas en el artículo 21, apartados 1 y 2, o

b) el acto jurídico sectorial de la Unión prevé el acceso inmediato, y cuando proceda automático y directo, a las notificaciones de incidentes por parte de los CSIRT, las autoridades competentes o los puntos de contacto únicos designados con arreglo a la presente Directiva y cuando los requisitos de notificación de incidentes significativos tengan un efecto al menos equivalente a los establecidos en el artículo 23, apartados 1 a 6 de la presente Directiva.

3. La Comisión, a más tardar el 17 de julio de 2023 proporcionará directrices aclaratorias de la aplicación de los apartados 1 y 2. La Comisión revisará dichas directrices periódicamente. Al elaborar dichas directrices, la Comisión tendrá en cuenta las observaciones del Grupo de Cooperación y la ENISA.

*Artículo 5*

**Armonización mínima**

La presente Directiva no será óbice para que los Estados miembros adopten o mantengan disposiciones que garanticen un nivel más elevado de ciberseguridad, siempre y cuando tales disposiciones sean compatibles con las obligaciones establecidas en el Derecho de la Unión.

*Artículo 6*

**Definiciones**

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

1) «sistemas de redes y de información»:

   a) una red de comunicaciones electrónicas tal como se definen en el 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, conforme a un programa, el tratamiento automático de datos digitales, o

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

2) «seguridad de los sistemas de redes y de información»: la capacidad de los sistemas de redes y de información de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos;

3) «ciberseguridad»: ciberseguridad tal como se define en el artículo 2, punto 1, del Reglamento (UE) 2019/881;

4) «estrategia nacional de ciberseguridad»: marco coherente de un Estado miembro que establece prioridades y objetivos estratégicos en el ámbito de la ciberseguridad y la gobernanza para alcanzarlos en dicho Estado miembro;

5) «cuasiincidente»: un hecho que habría podido comprometer la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos, pero cuya materialización completa se previno de manera satisfactoria o que no llegó a materializarse;

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

7) «incidente de ciberseguridad a gran escala»: 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;

8) «gestión de incidentes»: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un incidente o responder ante este y recuperarse de él;

9) «riesgo»: la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente;

10) «ciberamenaza»: una ciberamenaza tal como se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881;

11) «ciberamenaza significativa»: una ciberamenaza que, basándose en sus características técnicas, cabe suponer que tiene el potencial de provocar repercusiones graves en los sistemas de redes y de información de una entidad o para los usuarios de los servicios de la entidad causando perjuicios materiales o inmateriales considerables;

12) «producto de TIC»: un producto de TIC tal como se define en el artículo 2, punto 12, del Reglamento (UE) 2019/881;

13) «servicio de TIC»: un servicio de TIC tal como se define en el artículo 2, punto 13, del Reglamento (UE) 2019/881;

14) «proceso de TIC»: un proceso de TIC tal como se define en el artículo 2, punto 14, del Reglamento (UE) 2019/881;

15) «vulnerabilidad»: deficiencia, susceptibilidad o fallo de productos de TIC o servicios de TIC que puede ser aprovechado por una ciberamenaza;

16) «norma»: una norma tal como se define en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([29]);

17) «especificación técnica»: una especificación técnica tal como se define en el artículo 2, punto 4, del Reglamento (UE) n.º 1025/2012;

([29]) 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).

18) «punto de intercambio de internet»: una instalación de la red que permite interconectar más de dos redes independientes (sistemas autónomos), principalmente para facilitar el intercambio de tráfico de internet, que solo permite interconectar sistemas autónomos y que no requiere que el tráfico de internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, ni modifica ni interfiere de otra forma en dicho tráfico;

19) «sistema de nombres de dominio (DNS)»: un sistema de nombres distribuido jerárquicamente que posibilita la identificación de servicios y recursos de internet, permitiendo a los dispositivos de los usuarios finales utilizar servicios de enrutamiento y conectividad de internet para acceder a dichos servicios y recursos;

20) «proveedor de servicios de DNS»: una entidad que presta:

a) servicios a disposición pública de resolución recursiva de nombres de dominio para usuarios finales de internet, o

b) servicios de resolución autoritativa de nombres de dominio para uso por terceros, con excepción de los servidores raíz;

21) «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, independientemente de que cualquiera de esas operaciones sea realizada por la entidad o se haya externalizado, pero excluyendo las situaciones en las que los nombres de dominio de primer nivel sean utilizados por un registro únicamente para su propio uso;

22) «entidad que presta servicios de registro de nombres de dominio»: un registrador o un agente que actúe en nombre de los registradores, como un proveedor o revendedor de servicios de registro de privacidad o representación;

23) «servicio digital»: un servicio tal como se define en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([30]);

24) «servicio de confianza»: un servicio de confianza tal como se define en el artículo 3, punto 16, del Reglamento (UE) n.º 910/2014;

25) «prestador de servicios de confianza»: un prestador de servicios de confianza tal como se define en el artículo 3, punto 19, del Reglamento (UE) n.º 910/2014;

26) «servicio de confianza cualificado»: un servicio de confianza cualificado tal como se define en el artículo 3, punto 17, del Reglamento (UE) n.º 910/2014;

27) «prestador cualificado de servicios de confianza»: un prestador cualificado de servicios de confianza tal como se define en el artículo 3, punto 20, del Reglamento (UE) n.º 910/2014;

28) «mercado en línea»: un servicio digital tal como se define en el artículo 2, letra n), de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo ([31]);

29) «motor de búsqueda en línea»: un servicio digital tal como se define en el artículo 2, punto 5, del Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo ([32]);

30) «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 dichos recursos están distribuidos entre varias ubicaciones;

---

([30]) 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).

([31]) 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).

([32]) 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 las empresas que utilizan servicios de intermediación en línea (DO L 186 de 11.7.2019, p. 57).

31) «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;

32) «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;

33) «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, en particular, mediante chats, publicaciones, vídeos y recomendaciones;

34) «representante»: una persona física o jurídica establecida en la Unión que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios de DNS, un registro de nombres de dominio de primer nivel, una entidad que presta servicios de registro de nombres de dominio, un proveedor de servicios de computación en nube, un proveedor de servicios de centro de datos, un proveedor de redes de distribución de contenidos, un proveedor de servicios gestionados, un proveedor de servicios de seguridad gestionados, o un proveedor de un mercado en línea, de un motor de búsqueda en línea, o de plataformas de servicios de redes sociales que no esté establecido en la Unión, al que puede dirigirse una autoridad competente o un CSIRT en sustitución de la propia entidad, en lo que respecta a las obligaciones de dicha entidad con arreglo a la presente Directiva;

35) «entidad de la Administración pública»: una entidad reconocida como tal en un Estado miembro de conformidad con el Derecho nacional, excluidos el poder judicial, los parlamentos y los bancos centrales, que cumple los criterios siguientes:

   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 financiada mayoritariamente por el Estado, las autoridades regionales u otras entidades de Derecho público, su gestión se halla sometida a control por parte de esas autoridades o entidades, o tiene órganos de administración, de dirección o de supervisión más de la mitad de cuyos miembros los nombra el Estado, las autoridades regionales 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;

36) «red pública de comunicaciones electrónicas»: una red pública de comunicaciones electrónicas tal como se define en el artículo 2, punto 8, de la Directiva (UE) 2018/1972;

37) «servicio de comunicaciones electrónicas»: un servicio de comunicaciones electrónicas tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2018/1972;

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

39) «proveedor de servicios gestionados»: una entidad que presta servicios relacionados con la instalación, la gestión, la explotación o el mantenimiento de productos, redes, infraestructuras o aplicaciones de TIC o cualesquiera otros sistemas de redes y de información, a través de la asistencia o la administración activa, en las instalaciones de los clientes o a distancia;

40) «proveedor de servicios de seguridad gestionados»: un proveedor de servicios gestionados que lleva a cabo actividades relativas a la gestión de riesgos de ciberseguridad o presta asistencia para ello;

41) «organismo de investigación»: una entidad cuyo objetivo principal es llevar a cabo investigación aplicada o desarrollo experimental con vistas a explotar los resultados de dicha investigación con fines comerciales, excluidos los centros de enseñanza.

CAPÍTULO II

## MARCOS DE CIBERSEGURIDAD COORDINADOS

*Artículo 7*

### Estrategia nacional de ciberseguridad

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

a) objetivos y prioridades de la estrategia de ciberseguridad del Estado miembro que abarque, en particular, los sectores mencionados en los anexos I y II;

b) un marco de gobernanza para lograr los objetivos y prioridades mencionados en la letra a) del presente apartado, incluidas las políticas a que se refiere el apartado 2;

c) un marco de gobernanza que aclare las funciones y responsabilidades de las partes interesadas pertinentes a nivel nacional, que sustente la cooperación y la coordinación a nivel nacional entre las autoridades competentes, los puntos de contacto únicos y los CSIRT con arreglo a la presente Directiva, así como la coordinación y la cooperación entre dichos organismos y las autoridades competentes con arreglo a actos jurídicos sectoriales de la Unión;

d) un mecanismo para identificar los activos pertinentes y una evaluación de los riesgos de ciberseguridad en ese Estado miembro;

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

f) una lista de las diversas partes interesadas y autoridades que participan en la ejecución de la estrategia nacional de ciberseguridad;

g) un marco político para la coordinación reforzada entre las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2557 a efectos del intercambio de información sobre riesgos, ciberamenazas e incidentes así como sobre riesgos, amenazas e incidentes no relacionados con la ciberseguridad y el ejercicio de las funciones de supervisión, según proceda;

h) un plan, incluidas las medidas necesarias, para elevar el nivel general de concienciación de los ciudadanos en materia de ciberseguridad.

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

a) 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) sobre la inclusión y especificación de los requisitos en materia de ciberseguridad aplicables a los productos de TIC y los servicios de TIC en la contratación pública, incluidos los requisitos relativos a la certificación de ciberseguridad, al cifrado y al uso de productos de ciberseguridad de código abierto;

c) de gestión de las vulnerabilidades, incluidas la promoción y facilitación de una divulgación coordinada de vulnerabilidades con arreglo al artículo 12, apartado 1;

d) para mantener la disponibilidad general**,** la integridad y la confidencialidad del núcleo público de la internet abierta, incluida la ciberseguridad, cuando proceda, de los cables submarinos de comunicaciones;

e) de promoción del desarrollo y la integración de las tecnologías avanzadas pertinentes destinadas a aplicar medidas de gestión de riesgos de ciberseguridad de última generación;

f) de promoción y desarrollo de la educación y la formación en materia de ciberseguridad, capacidades de ciberseguridad, sensibilización e iniciativas de investigación y desarrollo, así como orientaciones sobre buenas prácticas y controles en materia de ciberhigiene, destinadas a los ciudadanos, las partes interesadas y las entidades;

g) de apoyo a las instituciones académicas y de investigación para el desarrollo, la mejora y la implantación de herramientas de ciberseguridad e infraestructuras de red seguras;

h) sobre los procedimientos pertinentes y las herramientas apropiadas para compartir información en apoyo del intercambio voluntario de información sobre ciberseguridad entre las entidades, de conformidad con el Derecho de la Unión;

i) de refuerzo de la ciberresiliencia y la base de referencia en materia de ciberhigiene de las pequeñas y medianas empresas, especialmente de las excluidas del ámbito de aplicación de la presente Directiva, proporcionando orientaciones y apoyo de fácil acceso para sus necesidades específicas;

j) de promoción de la ciberprotección activa.

3. Los Estados miembros notificarán sus estrategias nacionales de ciberseguridad a la Comisión en el plazo de tres meses a partir de su adopción. Los Estados miembros podrán excluir de tal notificación información relativa a su seguridad nacional.

4. Los Estados miembros evaluarán sus estrategias nacionales de ciberseguridad periódicamente y al menos cada cinco años en función de unos indicadores de rendimiento clave, y las actualizarán cuando proceda. La ENISA prestará asistencia los Estados miembros, cuando estos así lo soliciten, a la hora de elaborar o actualizar una estrategia nacional de ciberseguridad y de indicadores clave de rendimiento para su evaluación, con el fin de adaptarla a los requisitos y obligaciones establecidos en la presente Directiva.

*Artículo 8*

**Autoridades competentes y puntos de contacto únicos**

1. Cada Estado miembro designará o establecerá una o más autoridades competentes encargadas de la ciberseguridad y de las funciones de supervisión a que se refiere el capítulo VII (autoridades competentes).

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 o establecerá un punto de contacto único. Si un Estado miembro designa o establece únicamente una autoridad competente en virtud del apartado 1, 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 pertinentes en otros Estados miembros y, cuando proceda, con la Comisión y la ENISA, así como para garantizar la cooperación intersectorial con otras autoridades competentes dentro de su Estado miembro.

5. Los Estados miembros velarán por que sus autoridades competentes y puntos de contacto únicos dispongan de recursos adecuados para ejercer las funciones que les son asignadas de forma efectiva y eficiente y cumplir así los objetivos de la presente Directiva.

6. Cada Estado miembro notificará sin dilación indebida a la Comisión la identidad de la autoridad competente a que se refiere el apartado 1 y del punto de contacto único contemplado en el apartado 3, las tareas de dichas autoridades, y cualquier cambio de lo notificado que se introduzca posteriormente. Cada Estado miembro publicará la identidad de su autoridad competente. La Comisión hará pública la lista de puntos de contacto únicos.

*Artículo 9*

**Marcos nacionales de gestión de crisis de ciberseguridad**

1. Cada Estado miembro designará o establecerá una o varias autoridades competentes responsables de la gestión de incidentes y crisis de ciberseguridad a gran escala (autoridades de gestión de crisis de ciberseguridad). Los Estados miembros velarán por que esas autoridades dispongan de los recursos adecuados para llevar a cabo los cometidos que les son asignados de forma efectiva y eficiente. Los Estados miembros velarán por la coherencia con los marcos nacionales generales de gestión de crisis vigentes.

2. Cuando un Estado miembro designe o establezca más de una autoridad de gestión de crisis de ciberseguridad en virtud del apartado 1, indicará claramente cuál de dichas autoridades servirá de coordinador para la gestión de incidentes y crisis de ciberseguridad a gran escala.

3. 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.

4. Cada Estado miembro adoptará un plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala en el que se fijen los objetivos y las disposiciones de la gestión de los incidentes y las crisis de ciberseguridad a gran escala. Dicho plan establecerá, en particular:

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

b) las funciones y responsabilidades de las autoridades de gestión de crisis de ciberseguridad;

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 nacionales de preparación, incluidos los ejercicios y las actividades de formación;

e) las partes interesadas públicas y privadas pertinentes 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 su apoyo a ella.

5. En el plazo de tres meses a partir de la designación o el establecimiento de la autoridad de gestión de crisis de ciberseguridad a que se refiere el apartado 1, cada Estado miembro notificará a la Comisión la identidad de su autoridad y cualquier modificación posterior de esta. Los Estados miembros presentarán a la Comisión y a la red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe, por sus siglas en inglés) información pertinente relativa a los requisitos del apartado 4 sobre sus planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala en un plazo de tres meses a partir de la adopción de dichos planes. Los Estados miembros podrán excluir información cuando y en la medida en que sea necesario para su seguridad nacional.

*Artículo 10*

**Equipos de respuesta a incidentes de seguridad informática (CSIRT)**

1. Cada Estado miembro designará o establecerá uno o varios CSIRT. Los CSIRT podrán ser designados o establecidos en el marco de una autoridad competente. Los CSIRT cumplirán los requisitos establecidos en el artículo 11, apartado 1, cubrirán al menos los sectores, subsectores y tipos de entidades que figuran en los anexos I y II y se responsabilizarán de la gestión de incidentes de conformidad con un procedimiento claramente definido.

2. Los Estados miembros velarán por que cada CSIRT disponga de los recursos adecuados para llevar a cabo eficazmente sus cometidos, tal como se establece en el artículo 11, apartado 3.

3. Los Estados miembros velarán por que cada CSIRT tenga a su disposición una infraestructura de comunicación e información apropiada, segura y resiliente mediante la cual intercambiar información con las entidades esenciales e importantes y otras partes interesadas pertinentes. Para ello, los Estados miembros se asegurarán de que cada CSIRT contribuya 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 29 con comunidades sectoriales o intersectoriales de entidades esenciales e importantes.

5. Los CSIRT participarán en las revisiones interpares organizadas con arreglo al artículo 19.

6. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT.

7. Los CSIRT podrán establecer relaciones de cooperación con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países. Como parte de dichas relaciones de cooperación, los Estados miembros facilitarán un intercambio de información eficaz, eficiente y seguro con los equipos nacionales de respuesta a incidentes de seguridad informática de terceros países, utilizando los protocolos de intercambio de información pertinentes, incluido el protocolo TLP para el intercambio de información. Los CSIRT podrán intercambiar información pertinente con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países, incluidos datos personales de conformidad con la legislación de la Unión en materia de protección de datos.

8. Los CSIRT podrán cooperar con equipos nacionales de respuesta a incidentes de seguridad informática de terceros países u organismos equivalentes de terceros países, en particular con el fin de proporcionarles asistencia en materia de ciberseguridad.

9. Cada Estado miembros notificará sin dilación indebida a la Comisión la identidad del CSIRT a que se refiere el apartado 1 del presente artículo y el CSIRT designado coordinador en virtud del artículo 12, apartado 1, sus respectivas tareas desempeñadas en relación con las entidades esenciales e importantes y cualquier cambio en lo notificado que se introduzca posteriormente.

10. Los Estados miembros podrán solicitar la asistencia de la ENISA a la hora de crear sus CSIRT.

*Artículo 11*

**Obligaciones, capacidades técnicas y cometidos de los CSIRT**

1. Los CSIRT cumplirán los siguientes requisitos:

a) los CSIRT garantizarán una gran disponibilidad de sus canales de comunicación evitando los fallos puntuales simples y contarán con varios medios para ser contactado y contactar con otros en todo momento; 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 garantizarán la confidencialidad y fiabilidad de sus operaciones;

e) los CSIRT contarán con personal suficiente para garantizar la disponibilidad de sus servicios en todo momento y velarán por la adecuada formación de su personal;

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

Los CSIRT podrán participar en redes de cooperación internacional.

2. Los Estados miembros velarán por que sus CSIRT dispongan conjuntamente de las capacidades técnicas necesarias para llevar a cabo los cometidos a que se refiere el apartado 3. Los Estados miembros velarán por que se asignen a sus CSIRT recursos suficientes para garantizar unas dotaciones de personal adecuadas a fin de que los CSIRT puedan desarrollar sus capacidades técnicas.

3. Los CSIRT tendrán los siguientes cometidos:

a) realizar un seguimiento y analizar las ciberamenazas, las vulnerabilidades y los incidentes a escala nacional y, previa solicitud, prestar asistencia a las entidades esenciales e importantes afectadas por lo que respecta a la supervisión en tiempo real o cuasirreal de sus sistemas de redes y de información;

b) difundir alertas tempranas, alertas, avisos e información sobre las ciberamenazas, las vulnerabilidades y los incidentes entre las entidades esenciales e importantes afectadas, así como entre las autoridades competentes y otras partes interesadas pertinentes, a ser posible en tiempo cuasirreal;

c) responder a incidentes y prestar asistencia a las entidades esenciales e importantes afectadas, si procede;

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) proporcionar, a petición de una entidad esencial o importante afectada, una exploración proactiva de los sistemas de redes y de información de la entidad afectada para detectar vulnerabilidades que puedan tener una repercusión significativa;

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

g) cuando proceda, actuar como coordinador a efectos del proceso de divulgación coordinada de vulnerabilidades con arreglo al artículo 12, apartado 1;

h) contribuir al despliegue de herramientas seguras de intercambio de información en virtud del artículo 10, apartado 3.

Los CSIRT podrán llevar a cabo una exploración proactiva no intrusiva de los sistemas de redes y de información de acceso público de entidades esenciales e importantes. Dicha exploración se llevará a cabo para detectar sistemas de redes y de información vulnerables o configurados de forma insegura e informar a las entidades afectadas. Dicha exploración no tendrá ningún impacto negativo en el funcionamiento de los servicios de las entidades.

Al llevar a cabo los cometidos a que se refiere el párrafo primero, los CSIRT podrán dar prioridad a cometidos determinados sobre la base de un enfoque basado en el riesgo.

4. Los CSIRT establecerán relaciones de cooperación con partes interesadas pertinentes del sector privado, con vistas a mejorar la consecución de los objetivos de la presente Directiva.

5. A fin de facilitar la cooperación a que se refiere el apartado 4, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas, sistemas de clasificación y taxonomías en relación con:

a) los procedimientos de gestión de incidentes;

b) la gestión de crisis de ciberseguridad, y

c) la divulgación coordinada de las vulnerabilidades con arreglo al artículo 12, apartado 1.

*Artículo 12*

**Divulgación coordinada de las vulnerabilidades y una base de datos europea de vulnerabilidades**

1. Cada Estado miembro designará a uno de sus CSIRT como coordinador a efectos de la divulgación coordinada de las vulnerabilidades. El CSIRT designado como coordinador ejercerá de intermediario de confianza y facilitará, cuando sea necesario, la interacción entre la persona física o jurídica que notifique una vulnerabilidad y el fabricante o proveedor de los productos de TIC o los servicios de TIC potencialmente vulnerables, a petición de cualquiera de las partes. Los cometidos del CSIRT designado como coordinador incluirán:

a) identificar y contactar a las entidades afectadas;

b) prestar asistencia a las personas físicas o jurídicas que notifican una vulnerabilidad, y

c) negociar los plazos de divulgación y gestionar las vulnerabilidades que afectan a múltiples entidades.

Los Estados miembros velarán por que las personas físicas o jurídicas que así lo soliciten puedan notificar de forma anónima una vulnerabilidad al CSIRT designado como coordinador. El CSIRT designado como coordinador velará por que se lleve a cabo un seguimiento diligente de la vulnerabilidad notificada y garantizará el anonimato de la persona física o jurídica que notifique la vulnerabilidad. Cuando la vulnerabilidad notificada pueda repercutir significativamente en entidades de más de un Estado miembro, el CSIRT designado como coordinador de cada Estado miembro afectado cooperará, cuando proceda, con los demás CSIRT designados como coordinadores en el marco de la red de CSIRT.

2. La ENISA desarrollará y mantendrá, previa consulta con el Grupo de Cooperación, una base de datos europea de vulnerabilidades. Para ello, la ENISA establecerá y mantendrá los sistemas de información, las políticas y los procedimientos apropiados, y adoptará las medidas técnicas y organizativas necesarias para garantizar la seguridad y la integridad de la base de datos europea de vulnerabilidades, con vistas, en particular, a permitir que las entidades, con independencia de si están incluidas en el ámbito de aplicación de la presente Directiva y sus proveedores de sistemas de redes y de información divulguen y registren, de manera voluntaria, vulnerabilidades conocidas públicamente presentes en los productos de TIC o los servicios de TIC. Se facilitará a todas las partes interesadas acceso a la información sobre las vulnerabilidades que figura en la base de datos europea de vulnerabilidades. Dicha base de datos incluirá:

a) información que describa la vulnerabilidad;

b) los productos de TIC o los servicios de TIC afectados y la gravedad de la vulnerabilidad por lo que respecta a las circunstancias en que puede explotarse;

c) la disponibilidad de parches de seguridad asociados y, a falta de ellos, las orientaciones proporcionadas por las autoridades competentes o los CSIRT dirigidas a los usuarios de productos de TIC y los servicios de TIC vulnerables sobre la forma de reducir los riesgos derivados de las vulnerabilidades reveladas.

*Artículo 13*

**Cooperación a escala nacional**

1. Cuando sean distintos, las autoridades competentes, 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 CSIRT o, si procede, sus autoridades competentes, reciban las notificaciones sobre los incidentes significativos en virtud del artículo 23 y los incidentes, las ciberamenazas y los cuasiincidentes en virtud del artículo 30.

3. Los Estados miembros velarán por que sus CSIRT o, si procede, sus autoridades competentes informen a su punto de contacto único sobre las notificaciones de incidentes, ciberamenazas y cuasiincidentes presentadas en virtud de la presente Directiva.

4. Con el objetivo de garantizar que los cometidos y las obligaciones de las autoridades competentes, los puntos de contacto únicos y los CSIRT se cumplen de manera efectiva, los Estados miembros garantizarán, en la medida de lo posible, una cooperación adecuada entre dichos organismos y las autoridades encargadas de hacer cumplir la ley, las autoridades de protección de datos, las autoridades nacionales con arreglo a los Reglamentos (CE) n.º 300/2008 y (UE) 2018/1139, los organismos de supervisión con arreglo al Reglamento (UE) n.º 910/2014, las autoridades competentes con arreglo al Reglamento (UE) 2022/2554, las autoridades nacionales de reglamentación con arreglo a la Directiva (UE) 2018/1972, las autoridades competentes con arreglo a la Directiva (UE) 2022/2557, así como las autoridades competentes con arreglo a otros actos jurídicos sectoriales de la Unión en dicho Estado miembro.

5. Los Estados miembros velarán por que sus autoridades competentes con arreglo a la presente Directiva y sus autoridades competentes con arreglo a la Directiva (UE) 2022/2557 cooperen e intercambien periódicamente información sobre la identificación de entidades críticas, sobre los riesgos, las ciberamenazas y los incidentes así como sobre los riesgos, las amenazas y los incidentes no cibernéticos que afecten a entidades esenciales identificadas como entidades críticas con arreglo a la Directiva (UE) 2022/2557 y sobre las medidas adoptadas en respuesta a dichos riesgos, amenazas e incidentes. Los Estados miembros velarán asimismo porque sus autoridades competentes con arreglo a la presente Directiva y sus autoridades competentes con arreglo al Reglamento (UE) n.º 910/2014, al Reglamento (UE) 2022/2554 y a la Directiva (UE) 2018/1972 intercambien periódicamente la información pertinente, también en relación con incidentes y ciberamenazas pertinentes.

6. Los Estados miembros simplificarán la notificación a través de medios técnicos para las notificaciones a que se refieren los artículos 23 y 30.

CAPÍTULO III

**COOPERACIÓN A NIVEL DE LA UNIÓN E INTERNACIONAL**

*Artículo 14*

**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 cometidos con arreglo a los programas de trabajo bienales a que se refiere el apartado 7.

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 con arreglo al Reglamento (UE) 2022/2554 podrán participar en las actividades del Grupo de Cooperación de conformidad con el artículo 47, apartado 1, de dicho Reglamento.

Cuando proceda, el Grupo de Cooperación podrá invitar al Parlamento Europeo y 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 los siguientes cometidos:

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

b) proporcionar orientación a las autoridades competentes en relación con el desarrollo y la ejecución de políticas sobre divulgación coordinada de vulnerabilidades a que se refiere el artículo 7, apartado 2, letra c);

c) 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, la formación, los ejercicios y las habilidades, el desarrollo de capacidades, las normas y especificaciones técnicas, así como la identificación de entidades esenciales e importantes en virtud del artículo 2, apartado 2, letras b) a e);

d) intercambiar recomendaciones y cooperar con la Comisión en iniciativas políticas sobre aspectos emergentes de la ciberseguridad y la coherencia general de los requisitos sectoriales en este ámbito;

e) intercambiar recomendaciones y cooperar con la Comisión en la redacción de los actos delegados o de ejecución que adopte en virtud de la presente Directiva;

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

g) intercambiar puntos de vista sobre la aplicación de los actos jurídicos sectoriales de la Unión que contienen disposiciones sobre ciberseguridad;

h) si procede, analizar los informes sobre la revisión interpares a que se refiere el artículo 19, apartado 9, y extraer conclusiones y recomendaciones;

i) llevar a cabo evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas de conformidad con el artículo 22, apartado 1;

j) analizar casos de asistencia mutua, incluidas las experiencias y los resultados de las acciones transfronterizas de supervisión conjuntas a que se refiere el artículo 37;

k) a petición de uno o varios Estados miembros afectados, debatir las solicitudes específicas de asistencia mutua a que se refiere el artículo 37;

l) proporcionar orientación estratégica a la red de CSIRT y a EU-CyCLONe sobre cuestiones emergentes específicas;

m) intercambiar puntos de vista sobre la política relativa a las acciones de seguimiento tras incidentes y crisis de ciberseguridad a gran escala sobre la base de las lecciones extraídas de la red CSIRT y la EU-CyCLONe;

n) 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;

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

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

q) establecer la metodología y los aspectos organizativos de las revisiones interpares a que se refiere el artículo 19, apartado 5, así como establecer la metodología de autoevaluación para los Estados miembros de conformidad con el artículo 19, apartado 5, con la ayuda de la Comisión y de la ENISA y, en cooperación con la Comisión y la ENISA, elaborar códigos de conducta que respalden los métodos de trabajo de los expertos en ciberseguridad designados de conformidad con el artículo 19, apartado 6;

r) preparar informes a efectos de la revisión que contempla el artículo 40 sobre la experiencia adquirida a nivel estratégico y con las revisiones interpares;

s) debatir y llevar a cabo una evaluación periódica de la situación de las ciberamenazas o incidentes, como los programas de secuestro.

El Grupo de Cooperación presentará los informes a que se refiere el párrafo primero, letra r), a la Comisión, al Parlamento Europeo y al Consejo.

5. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus representantes en el Grupo de Cooperación.

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

7. A más tardar el 1 de febrero de 2024 y cada dos años a partir de entonces, el Grupo de Cooperación elaborará un programa de trabajo sobre las acciones que deben emprenderse para llevar a la práctica sus objetivos y cometidos.

8. 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 39, apartado 2.

La Comisión intercambiará asesoramiento y cooperará con el Grupo de Cooperación sobre los proyectos de actos de ejecución a que se refiere el párrafo primero del presente apartado, de conformidad con el apartado 4, letra e).

9. El Grupo de Cooperación se reunirá periódicamente, y en cualquier caso por lo menos una vez al año, con el Grupo de resiliencia de las entidades críticas establecido con arreglo a la Directiva (UE) 2022/2557 para promover y facilitar la cooperación estratégica y el intercambio de información.

*Artículo 15*

**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 nacional de CSIRT.

2. La red de CSIRT estará formada por representantes de los CSIRT designados o establecidos en virtud del artículo 10 y el Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión (CERT-EU por sus siglas en inglés). La Comisión participará en la red de CSIRT en calidad de observador. La ENISA se hará cargo de la secretaría y prestará asistencia activamente para la cooperación entre los CSIRT.

3. La red de CSIRT llevará a cabo los siguientes cometidos:

a) intercambiar información sobre las capacidades de los CSIRT;

b) facilitar la puesta en común, la transferencia y el intercambio de tecnología y las medidas, las políticas, los instrumentos, los procedimientos, las mejores prácticas y los marcos pertinentes entre los CSIRT;

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

d) intercambiar información sobre publicaciones y recomendaciones en materia en materia de ciberseguridad;

e) garantizar la interoperabilidad en lo que respecta a las especificaciones y protocolos de intercambio de información;

f) 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;

g) 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;

h) prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos en virtud de la presente Directiva;

i) cooperar, intercambiar mejores prácticas y prestar asistencia a los CSIRT designados como coordinadores en virtud del artículo 12, apartado 1, en lo que respecta a la gestión de la divulgación coordinada de vulnerabilidades que puedan tener una repercusión significativa en entidades de más de un Estado miembro;

j) debatir e identificar 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 disposiciones de coordinación en respuesta a riesgos e incidentes transfronterizos;

   v) la contribución al plan nacional de respuesta a incidentes y crisis de ciberseguridad a gran escala a que se refiere el artículo 9, apartado 4, a petición de un Estado miembro;

k) 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 j), y solicitar, cuando sea necesario, directrices a este respecto;

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

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

n) 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 ciberamenazas en toda la Unión;

o) si procede, debatir los informes sobre la revisión interpares a que se refiere el artículo 19, apartado 9;

p) proporcionar 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 más tardar el 17 de enero de 2025, y posteriormente cada dos años, la red de CSIRT evaluará, a efectos de la revisión a que se refiere el artículo 40, los progresos realizados en relación con la cooperación operativa y adoptará un informe. Concretamente, el informe extraerá conclusiones y recomendaciones sobre la base de los resultados de las revisiones interpares a que se refiere el artículo 19, que se llevan a cabo en relación con los CSIRT nacionales. Dicho informe se enviará al Grupo de Cooperación.

5. La red de CSIRT adoptará su reglamento interno.

6. La red de CSIRT y la EU-CyCLONe acordarán disposiciones de procedimiento y cooperarán sobre la base de dichas disposiciones.

*Artículo 16*

**Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe)**

1. Se crea EU-CyCLONe a fin de 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 relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión.

2. EU-CyCLONe estará formada por representantes de las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y, en los casos en que un incidente de ciberseguridad a gran escala potencial o en curso tenga o pueda tener un impacto significativo en los servicios y actividades incluidos en el ámbito de aplicación de la presente Directiva, la Comisión. En otros casos, la Comisión participará en las actividades de EU-CyCLONe en calidad de observador.

La ENISA se hará cargo de la secretaría de EU-CyCLONe, promoverá el intercambio seguro de información y facilitará las herramientas necesarias al objeto de respaldar 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 en calidad de observadores.

3. Los cometidos de EU-CyCLONe serán los 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 de los incidentes y crisis de ciberseguridad a gran escala;

c) evaluar las consecuencias y las repercusiones de los incidentes y crisis de ciberseguridad a gran escala pertinentes y proponer posibles medidas paliativas;

d) coordinar la gestión de incidentes y crisis de ciberseguridad a gran escala y servir de apoyo en la toma de decisiones a nivel político en relación con tales incidentes y crisis;

e) examinar, a petición de un Estado miembro afectado, los planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala a que se refiere el artículo 9, apartado 4.

4. EU-CyCLONe adoptará su reglamento interno.

5. EU-CyCLONe informará periódicamente al Grupo de Cooperación de la gestión de los incidentes y las crisis de ciberseguridad a gran escala, así como de las tendencias, 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 que prevé el artículo 15, apartado 6.

7. A más tardar el 17 de julio de 2024 y posteriormente cada dieciocho meses, EU-CyCLONe presentará al Parlamento Europeo y al Consejo un informe de evaluación de su labor.

*Artículo 17*

**Cooperación internacional**

De conformidad con el artículo 218 del TFUE, la Unión podrá celebrar, en su caso, acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen la participación de estos en determinadas actividades del Grupo de Cooperación, la red de CSIRT y EU-CyCLONe. Dichos acuerdos cumplirán el Derecho de la Unión en materia de protección de datos.

*Artículo 18*

**Informe sobre la situación de la ciberseguridad en la Unión**

1. La ENISA adoptará, en cooperación con la Comisión y el Grupo de Cooperación, un informe bienal sobre la situación de la ciberseguridad en la Unión y remitirá y presentará ese informe al Parlamento Europeo. El informe estará disponible, entre otras formas, como datos legibles por máquina, y en él se recogerán los siguientes aspectos:

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

b) una evaluación del desarrollo de las capacidades de ciberseguridad en los sectores público y privado en toda la Unión;

c) una evaluación del nivel general de sensibilización en materia de ciberseguridad y ciberhigiene entre los ciudadanos y las empresas, incluidas las pequeñas y medianas empresas;

d) una evaluación agregada de los resultados de las revisiones interpares contempladas en el artículo 19;

e) una evaluación agregada del nivel de madurez de las capacidades y los recursos de ciberseguridad en toda la Unión, también los de nivel sectorial, así como de la medida en que las estrategias nacionales de ciberseguridad de los Estados miembros están armonizadas.

2. El informe incluirá recomendaciones políticas concretas con vistas a abordar las deficiencias e 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 en materia de incidentes y ciberamenazas preparados por la ENISA de conformidad con el artículo 7, apartado 6, del Reglamento (UE) 2019/881.

3. La ENISA, en cooperación con la Comisión, el Grupo de Cooperación y la red de CSIRT, desarrollará la metodología, en particular las variables pertinentes, como los indicadores cuantitativos y cualitativos, de la evaluación agregada mencionada en el apartado 1, letra e).

*Artículo 19*

**Revisiones interpares**

1. El Grupo de Cooperación, a más tardar el 17 de enero de 2025, establecerá, con la ayuda de la Comisión y de la ENISA y, cuando proceda, de la red de CSIRT, la metodología y los aspectos organizativos de las revisiones interpares con vistas a aprender de las experiencias compartidas, reforzar la confianza mutua, lograr un elevado nivel común de ciberseguridad y mejorar las capacidades y políticas de ciberseguridad de los Estados miembros necesarias para la aplicación de la presente Directiva. La participación en las revisiones interpares será voluntaria. Las revisiones interpares serán realizadas por expertos en ciberseguridad. Los expertos en ciberseguridad serán designados por al menos dos Estados miembros distintos del Estado miembro objeto de revisión.

Las revisiones interpares abarcarán, por lo menos, uno de los siguientes aspectos:

a) el nivel de aplicación de las medidas para la gestión de riesgos de ciberseguridad y las obligaciones de notificación establecidas en los artículos 21 y 23;

b) el nivel de capacidades, incluidos los recursos financieros, técnicos y humanos disponibles, y la eficacia con que las autoridades competentes han llevado a cabo sus cometidos;

c) las capacidades operativas de los CSIRT;

d) el nivel de aplicación de la asistencia mutua a que se refiere el artículo 37;

e) el nivel de aplicación de los mecanismos para el intercambio de información sobre ciberseguridad a que se refiere el artículo 29;

f) problemas específicos de carácter transfronterizo o intersectorial.

2. La metodología contemplada en el apartado 1 abarcará criterios objetivos, no discriminatorios, justos y transparentes que los Estados miembros utilizarán para designar los expertos en ciberseguridad admisibles para realizar las revisiones interpares. La Comisión y la ENISA participarán en las revisiones interpares en calidad de observadores.

3. Los Estados miembros podrán definir los problemas específicos mencionados en el apartado 1, letra f), a los fines de la revisión interpares.

4. Antes del inicio de la revisión interpares como se menciona en el apartado 1, los Estados miembros comunicarán a los Estados miembros participantes su alcance, incluidos los problemas específicos definidos en virtud del apartado 3.

5. Antes del inicio de la revisión interpares, los Estados miembros podrán llevar a cabo una autoevaluación de los aspectos revisados y facilitarla a los expertos en ciberseguridad designados. El Grupo de Cooperación, con la asistencia de la Comisión y de la ENISA, establecerá la metodología para la autoevaluación de los Estados miembros.

6. Las revisiones interpares conllevarán visitas *in situ* presenciales o virtuales e intercambios de información a distancia. En consonancia con el principio de buena cooperación, el Estado miembro objeto de la revisión interpares facilitará a los expertos en ciberseguridad designados la información necesaria para la evaluación, sin perjuicio del Derecho de la Unión o nacional relativo a la protección de la información confidencial o clasificada ni de la salvaguardia de las funciones esenciales del Estado, como la seguridad nacional. El Grupo de Cooperación, en cooperación con la Comisión y la ENISA, elaborará códigos de conducta adecuados que sustenten los métodos de trabajo de los expertos en ciberseguridad designados. Cualquier información obtenida a través de la revisión interpares se utilizará exclusivamente para tal finalidad. Los expertos en ciberseguridad que participen en la revisión interpares no divulgarán a terceros ninguna información sensible o confidencial obtenida en el transcurso de dicha revisión interpares.

7. Una vez sean objeto de una revisión interpares, los mismos aspectos revisados en un Estado miembro no serán objeto de una revisión interpares ulterior en ese Estado miembro durante los dos años siguientes a la conclusión de la revisión interpares, a menos que lo solicite el Estado miembro o se acuerde tras una propuesta del Grupo de Cooperación.

8. Los Estados miembros velarán por que cualquier riesgo de conflicto de intereses que afecte a los expertos en ciberseguridad designados se comunique a los otros Estados miembros, al Grupo de Cooperación, a la Comisión y a la ENISA antes del inicio de la revisión interpares. El Estado miembro objeto de la revisión interpares podrá oponerse a la designación de determinados expertos en ciberseguridad por motivos debidamente justificados que se comunicarán al Estado miembro que los designe.

9. Los expertos en ciberseguridad que participen en revisiones interpares elaborarán informes sobre las constataciones y conclusiones de las revisiones. Los Estados miembros objeto de revisión interpares podrán formular observaciones sobre los proyectos de informe que les conciernan, que se adjuntarán a los informes. Los informes incluirán recomendaciones que permitan la mejora de los aspectos que abarque la revisión interpares. Los informes se remitirán al Grupo de Cooperación y la red de CSIRT cuando proceda. Un Estado miembro objeto de revisión interpares podrá decidir poner a disposición del público su informe, o una versión editada del mismo.

## CAPÍTULO IV

## MEDIDAS PARA LA GESTIÓN DE RIESGOS DE CIBERSEGURIDAD Y OBLIGACIONES DE NOTIFICACIÓN

### *Artículo 20*

### Gobernanza

1. Los Estados miembros velarán por que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas para la gestión de riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 21, supervisen su puesta en práctica y respondan por el incumplimiento por parte de las entidades de dicho artículo.

La aplicación del presente apartado se entenderá sin perjuicio del Derecho nacional relativo a las normas sobre responsabilidad aplicables a las instituciones públicas, así como a la responsabilidad de los funcionarios públicos y los cargos electos o designados.

2. Los Estados miembros garantizarán que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.

*Artículo 21*

**Medidas para la gestión de riesgos de ciberseguridad**

1. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

Teniendo en cuenta la situación y, en su caso, las normas europeas e internacionales pertinentes, así como el coste de su aplicación, las medidas a que se refiere el párrafo primero garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado en relación con los riesgos planteados. Al evaluar la proporcionalidad de dichas medidas, se tendrá debidamente en cuenta el grado de exposición de la entidad a los riesgos, el tamaño de la entidad y la probabilidad de que se produzcan incidentes y su gravedad, incluidas sus repercusiones sociales y económicas.

2. Las medidas a que se hace referencia en el apartado 1 se fundamentarán en un enfoque basado en todos los peligros que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a incidentes, e 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;

c) la continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, 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;

e) la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida 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) las prácticas básicas de ciberhigiene y formación en ciberseguridad;

h) las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;

i) la seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;

j) el uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

3. Los Estados miembros velarán por que, al estudiar la idoneidad de las medidas a que se refiere el apartado 2, letra d), del presente artículo, las entidades tengan 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, al estudiar la idoneidad de las medidas a que se refiere el apartado 2, letra d), las entidades deban tener en cuenta los resultados de las evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas realizadas de conformidad con el artículo 22, apartado 1.

4. Los Estados miembros se asegurarán de que cuando una entidad constate que no cumple las medidas previstas en el apartado 2, adopte, sin demora indebida, todas las medidas correctoras apropiadas y proporcionadas necesarias.

5. A más tardar el 17 de octubre de 2024, la Comisión adoptará actos de ejecución por los que se establezcan los requisitos técnicos y metodológicos de las medidas a que se refiere el apartado 2 con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza.

La Comisión podrá adoptar actos de ejecución en los que se establezcan los requisitos técnicos y metodológicos, así como los requisitos sectoriales, según proceda, de las medidas a que se refiere el apartado 2 con respecto a las entidades esenciales e importantes distintas de las mencionadas en el párrafo primero del presente apartado.

Al elaborar los actos de ejecución a que se refieren los párrafos primero y segundo del presente apartado, la Comisión seguirá, en la mayor medida de lo posible, las normas europeas e internacionales, así como las especificaciones técnicas pertinentes. La Comisión intercambiará asesoramiento y colaborará con el Grupo de Cooperación y la ENISA acerca de los proyectos de actos de ejecución de conformidad con el artículo 14, apartado 4, letra e).

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 39, apartado 2.

*Artículo 22*

**Evaluaciones coordinadas de los riesgos de seguridad de las cadenas de suministro críticas a escala de la Unión**

1. El Grupo de Cooperación, en colaboración con la Comisión y la ENISA, podrá 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 y, en caso necesario, con las partes interesadas pertinentes, delimitará los servicios, sistemas o productos de TIC críticos específicos que podrán ser objeto de la evaluación coordinada de riesgos de seguridad a que se refiere el apartado 1.

*Artículo 23*

**Obligaciones de notificación**

1. Cada Estado miembro velará por que las entidades esenciales e importantes notifiquen, sin demora indebida, a su CSIRT o, en su caso, a su autoridad competente de conformidad con el apartado 4 cualquier incidente que tenga un impacto significativo en la prestación de sus servicios según se contempla en el apartado 3 (incidente significativo). Cuando proceda, las entidades afectadas notificarán, sin demora indebida, a los destinatarios de sus servicios los incidentes significativos susceptibles de afectar negativamente a la prestación de dichos servicios. Cada Estado miembro garantizará que dichas entidades notifiquen, entre otros detalles, cualquier información que permita al CSIRT o, en su caso, a la autoridad competente determinar las repercusiones transfronterizas del incidente. El mero acto de notificar no elevará la responsabilidad de la entidad notificante.

Cuando las entidades afectadas notifiquen a la autoridad competente un incidente significativo con arreglo al párrafo primero, el Estado miembro velará por que dicha autoridad competente transmita la notificación al CSIRT en el momento de su recepción.

En caso de un incidente significativo transfronterizo o intersectorial, los Estados miembros velarán por que se facilite a sus puntos de contacto únicos, a su debido tiempo, la información pertinente notificada de conformidad con el apartado 4.

2. Cuando proceda, los Estados miembros garantizarán que las entidades esenciales e importantes comuniquen, sin demora indebida, a los destinatarios de sus servicios que puedan verse afectados por una ciberamenaza significativa las medidas o soluciones que dichos destinatarios pueden aplicar en respuesta a la amenaza. Cuando proceda, las entidades notificarán asimismo la propia ciberamenaza significativa a esos destinatarios.

3. Un incidente se considerará significativo si:

a) ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada;

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

4. Los Estados miembros velarán por que, a los efectos de la notificación con arreglo al apartado 1, las entidades afectadas presenten al CSIRT o, en su caso, a la autoridad competente:

a) sin demora indebida y, en cualquier caso, en el plazo de veinticuatro horas desde que se haya tenido constancia del incidente significativo, una alerta temprana en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada o puede tener repercusiones transfronterizas;

b) sin demora indebida y, en cualquier caso, en el plazo de setenta y dos horas desde que se haya tenido constancia del incidente significativo, una notificación del incidente en la que se actualizará, cuando proceda, la información contemplada en la letra a) y se expondrá una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles;

c) a instancias de un CSIRT o, en su caso, de la autoridad competente, un informe intermedio con las actualizaciones pertinentes sobre la situación;

d) un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos:

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

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

   iii) las medidas paliativas aplicadas y en curso;

   iv) cuando proceda, las repercusiones transfronterizas del incidente;

e) en el caso de que el incidente siga en curso en el momento de la presentación del informe final contemplado en la letra d), los Estados miembros velarán por que las entidades afectadas presenten un informe de situación en ese momento y un informe final en el plazo de un mes a partir de que hayan gestionado el incidente.

Como excepción a lo dispuesto en la letra b) del párrafo primero, un prestador de servicios de confianza, con respecto a los incidentes significativos que afecten a la prestación de sus servicios de confianza, lo notificará al CSIRT o, en su caso, a la autoridad competente, sin demora indebida y, en cualquier caso, en un plazo de veinticuatro horas desde que haya tenido constancia del incidente significativo.

5. El CSIRT o la autoridad competente ofrecerá, sin demora indebida y, cuando sea posible, en el plazo de veinticuatro horas tras la recepción de la alerta temprana a que se refiere el apartado 4, letra a), una respuesta a la entidad notificante, en particular sus comentarios iniciales sobre el incidente significativo y, a instancias de la entidad, una orientación o asesoramiento operativo sobre la aplicación de posibles medidas paliativas. Cuando el CSIRT no sea el destinatario inicial de 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, el CSIRT o la autoridad competente también proporcionará orientación a efectos de denunciar el incidente significativo ante las autoridades encargadas de hacer cumplir la ley.

6. Cuando proceda, y en particular si el incidente significativo afecta a dos o más Estados miembros, el CSIRT, la autoridad competente o el punto de contacto único al que se haya notificado el incidente significativo informará de este, sin demora indebida, a los demás Estados miembros afectados y a la ENISA. Dicha información incluirá el tipo de información recibida de conformidad con el apartado 4. Al hacerlo, los CSIRT, las autoridades competentes o los puntos de contacto únicos preservarán, de conformidad con el Derecho de la Unión o nacional, 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 significativo o hacer frente a un incidente significativo en curso, o cuando la divulgación del incidente significativo redunde en el interés público, el CSIRT de un Estado miembro o, si procede, su autoridad competente y, en su caso, los CSIRT o las autoridades competentes de otros Estados miembros afectados, podrán informar al público, después de consultarlo con la entidad afectada, del incidente significativo o exigir a la entidad que lo haga.

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

9. El punto de contacto único presentará cada tres meses a la ENISA un informe de síntesis que incluya datos anonimizados y agregados sobre los incidentes significativos, los incidentes, las ciberamenazas y los cuasiincidentes notificados de conformidad con el apartado 1 del presente artículo y con el artículo 30. A fin de facilitar el suministro de información comparable, la ENISA podrá adoptar 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. Los CSIRT o, en su caso, las autoridades competentes facilitarán a las autoridades competentes designadas con arreglo a la Directiva (UE) 2022/2557 información sobre los incidentes significativos, los incidentes, las ciberamenazas y los cuasiincidentes notificados de conformidad con el apartado 1 del presente artículo y con el artículo 30 por entidades equivalentes a entidades críticas conforme a lo dispuesto en la Directiva (UE) 2022/2557

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 el apartado 1 del presente artículo y con el artículo 30, y de una comunicación remitida con arreglo al apartado 2 del presente artículo.

A más tardar el 17 de octubre de 2024, la Comisión, con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, adoptará actos de ejecución en los que se especifiquen en mayor medida los casos en los que un incidente se considerará significativo, tal como se contempla en el apartado 3. La Comisión podrá adoptar tales actos de ejecución con respecto a otras entidades esenciales e importantes.

La Comisión intercambiará asesoramiento y colaborará con el Grupo de Cooperación acerca de los proyectos de actos de ejecución a que se refieren los párrafos primero y segundo del presente apartado, de conformidad con el artículo 14, apartado 4, letra e).

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 39, apartado 2.

*Artículo 24*

**Utilización de esquemas europeos de certificación de la ciberseguridad**

1. A los efectos de demostrar la conformidad con determinados requisitos del artículo 21, los Estados miembros podrán exigir a las entidades esenciales e importantes que utilicen productos, servicios y procesos de TIC particulares, desarrollados por la entidad esencial o importante o adquiridos a terceros, que estén certificados en virtud de un esquema europeo de certificación de la ciberseguridad adoptado en virtud del artículo 49 del Reglamento (UE) 2019/881. Asimismo, los Estados miembros promoverán que las entidades esenciales e importantes utilicen servicios de confianza cualificados.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, por los que se complete la presente Directiva especificando qué categorías de entidades esenciales e importantes están obligadas a utilizar determinados productos, servicios o procesos de TIC certificados o a obtener una certificación en virtud de un esquema europeo de certificación de la ciberseguridad en virtud del artículo 49 del Reglamento (UE) 2019/881. Dichos actos delegados se adoptarán cuando se hayan detectado niveles insuficientes de ciberseguridad, e incluirán un período de ejecución.

Antes de adoptar dichos actos delegados, la Comisión llevará a cabo una evaluación de impacto, así como consultas de conformidad con el artículo 56 del Reglamento (UE) 2019/881.

3. Cuando no se disponga de un esquema europeo de certificación de la ciberseguridad apropiado a los efectos del apartado 2 del presente artículo, la Comisión, previa consulta al Grupo de Cooperación y al Grupo Europeo de Certificación de la Ciberseguridad, podrá solicitar a la ENISA que prepare una propuesta de esquema en virtud del artículo 48, apartado 2, del Reglamento (UE) 2019/881.

*Artículo 25*

**Normalización**

1. A fin de promover una aplicación convergente de lo dispuesto en el artículo 21, 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 técnicas europeas e internacionales que sean pertinentes en materia de seguridad de los sistemas de redes y de información.

2. La ENISA, en colaboración con los Estados y, cuando corresponda, tras consultar a las partes interesadas correspondientes, 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 que permitirían cubrir esas áreas.

CAPITULO V

**JURISDICCIÓN Y REGISTRO**

*Artículo 26*

**Jurisdicción y territorialidad**

1. Las entidades comprendidas en el ámbito de aplicación de la presente Directiva se considerarán sometidas a la jurisdicción del Estado miembro en el que están establecidas, salvo en el caso de:

a) los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público, que se considerarán sometidos a la jurisdicción del Estado miembro en el que prestan sus servicios;

b) los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea o de plataformas de servicios de redes sociales, que se considerarán sometidos a la jurisdicción del Estado miembro en el que se encuentre su establecimiento principal en la Unión con arreglo al apartado 2;

c) las entidades de la Administración pública, que se considerarán sometidas a la jurisdicción del Estado miembro que las haya establecido.

2. A los efectos de la presente Directiva, se considerará que una entidad de las contempladas en el apartado 1, letra b), tiene su establecimiento principal en la Unión 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. Si no puede determinarse dicho Estado miembro o si dichas decisiones no se toman en la Unión, se considerará que el establecimiento principal se encuentra en el Estado miembro en el que se lleven a cabo las operaciones de ciberseguridad. Si no puede determinarse dicho Estado miembro, se considerará que el establecimiento principal se encuentra en el Estado miembro en el que la entidad de que se trate tenga el establecimiento con mayor número de trabajadores en la Unión.

3. Si una entidad de las contempladas en el apartado 1, letra b), 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 dentro de la Unión designado con arreglo al presente apartado, cualquier Estado miembro en el que la entidad preste servicios podrá emprender acciones legales contra la entidad por incumplimiento de la presente Directiva.

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

5. Los Estados miembros que hayan recibido una solicitud de asistencia mutua en relación con una entidad de las contempladas en el apartado 1, letra b), podrán, dentro de los límites de dicha solicitud, adoptar las medidas de supervisión y ejecución adecuadas en relación con la entidad en cuestión que presta servicios o que tiene los sistemas de redes y de información en su territorio.

*Artículo 27*

**Registro de entidades**

1. La ENISA creará y mantendrá un registro de los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, las entidades que prestan servicios de registro de nombres de dominio, 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, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, sobre la base de la información recibida de los puntos de contacto únicos de conformidad con el apartado 4. Previa solicitud, la ENISA permitirá el acceso de las autoridades competentes a ese registro, garantizando al mismo tiempo que se protege la confidencialidad de la información, cuando proceda.

2. Los Estados miembros exigirán a las entidades a que se refiere el apartado 1, que presenten a más tardar 17 de enero de 2025 la siguiente información a las autoridades competentes:

a) el nombre de la entidad;

b) el sector, subsector y tipo de entidad a que se refieren los anexos I o II, en su caso;

c) la dirección del establecimiento principal de la entidad 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 26, apartado 3;

d) los datos de contacto actualizados, en particular las direcciones de correo electrónico y los números de teléfono de la entidad y, en su caso, de su representante designado en virtud del artículo 26, apartado 3;

e) los Estados miembros en los que la entidad presta servicios, y

f) los rangos de IP de la entidad.

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

4. Tras recibir la información a que se refieren los apartados 2 y 3, salvo la contemplada en el apartado 2, letra f), el punto de contacto único del Estado miembro afectado transmitirá sin demora indebida a la ENISA dicha información.

5. Cuando proceda, la información contemplada en los apartados 2 y 3 del presente artículo se transmitirá mediante los mecanismos nacionales mencionados en el artículo 3, apartado 4, párrafo cuarto.

*Artículo 28*

**Base de datos sobre el registro de nombres de dominio**

1. A efectos de contribuir a la seguridad, estabilidad y resiliencia del DNS, los Estados miembros exigirán que los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio 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 el Derecho de la Unión en materia de protección de datos por lo que respecta a los datos de carácter personal.

2. A los efectos del apartado 1, los Estados miembros exigirán que la base de datos sobre el registro de nombres de dominio contenga la información necesaria para identificar y contactar con los titulares de los nombres de dominio y los puntos de contacto que administran los nombres de dominio en los dominios de primer nivel. Dicha información incluirá los elementos siguientes:

a) el nombre del dominio;

b) la fecha de registro;

c) el nombre del solicitante, su dirección de correo electrónico de contacto y su número de teléfono;

d) la dirección de correo electrónico de contacto y el número de teléfono del punto de contacto que administra el nombre de dominio en caso de que no sean los del solicitante.

3. Los Estados miembros exigirán que los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio cuenten con políticas y procedimientos, incluidos procedimientos de verificación, para garantizar que las bases de datos contempladas en el apartado 1 incluyan información precisa y completa. Los Estados miembros exigirán que tales políticas y procedimientos se hagan públicos.

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

5. Los Estados miembros exigirán que los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio 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 el Derecho de la Unión en materia de protección de datos. Los Estados miembros exigirán que los registros de nombres de dominio de primer nivel y las entidades que prestan servicios de registro de nombres de dominio respondan sin demora indebida y, en cualquier caso, en un plazo de setenta y dos horas desde la recepción de la solicitud de acceso. Los Estados miembros exigirán que las políticas y los procedimientos de divulgación de dichos datos se hagan públicos.

6. El cumplimiento de las obligaciones establecidas en los apartados 1 a 5 no dará lugar a una duplicación de la recopilación de datos de registro de nombres de dominio. A tal fin, los Estados miembros exigirán a los registros de nombres de dominio de primer nivel y a las entidades que prestan servicios de registro de nombres de dominio que cooperen entre sí.

## CAPÍTULO VI

## INTERCAMBIO DE INFORMACIÓN

*Artículo 29*

### Mecanismos de intercambio de información sobre ciberseguridad

1. Los Estados miembros velarán por que las entidades comprendidas en el ámbito de aplicación de la presente Directiva y, cuando proceda, otras entidades no comprendidas en el ámbito de aplicación de la presente Directiva puedan intercambiar entre sí de forma voluntaria información relevante sobre ciberseguridad, en particular la relativa a ciberamenazas, cuasiincidentes, vulnerabilidades, técnicas y procedimientos, indicadores de compromiso, tácticas de los adversarios, información específica del agente de riesgo, alertas de ciberseguridad y recomendaciones sobre configuraciones de las herramientas de seguridad para detectar ciberataques, siempre que dicho intercambio de información:

a) se haga con el objetivo de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión;

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, contención y prevención de amenazas, estrategias de mitigación, o etapas de respuesta y recuperación, o al fomentar la investigación de ciberamenazas en colaboración con entidades públicas y privadas.

2. Los Estados miembros garantizarán que el intercambio de información se desarrolle dentro de comunidades de entidades esenciales e importantes y, cuando proceda, sus proveedores o prestadores de servicios. Dicho intercambio se pondrá en práctica a través de mecanismos de intercambio de información sobre ciberseguridad que respeten la posible naturaleza delicada de la información compartida.

3. Los Estados miembros facilitarán el establecimiento de los mecanismos de intercambio de información sobre ciberseguridad a que se refiere el apartado 2 del presente artículo. Dichos mecanismos podrán precisar los elementos operativos, incluido el uso de plataformas de TIC específicas y de herramientas de automatización, el contenido y las condiciones de los mecanismos de intercambio de información. Al establecer los detalles de la participación de las autoridades públicas en los mecanismos mencionados, los Estados miembros podrán imponer condiciones sobre la información puesta a disposición por las autoridades competentes o los CSIRT. Los Estados miembros ofrecerán apoyo a la aplicación de dichos mecanismos de conformidad con las correspondientes políticas a que se refiere el artículo 7, apartado 2, letra h).

4. Los Estados miembros velarán por que las entidades esenciales e importantes notifiquen a las autoridades competentes su participación en los mecanismos de intercambio de información sobre ciberseguridad 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 intercambio de buenas prácticas y facilitando orientación.

*Artículo 30*

**Notificación voluntaria de información pertinente**

1. Los Estados miembros velarán por que, además de las obligaciones de notificación previstas en el artículo 23, las notificaciones puedan ser presentadas a los CSIRT o, en su caso, a las autoridades competentes, de forma voluntaria, por:

a) las entidades esenciales e importantes en el caso de incidentes, ciberamenazas y cuasiincidentes;

b) las entidades distintas de las mencionadas en la letra a), independientemente de si están o no comprendidas en el ámbito de aplicación de la presente Directiva, en el caso de incidentes, ciberamenazas o cuasiincidentes significativos.

2. Los Estados miembros tramitarán las notificaciones contempladas en el apartado 1 del presente artículo de conformidad con el procedimiento establecido en el artículo 23. Los Estados miembros podrán dar prioridad a la tramitación de notificaciones obligatorias sobre las notificaciones voluntarias.

Cuando sea necesario, los CSIRT y, cuando proceda, las autoridades competentes, proporcionarán a los puntos de contacto únicos la información sobre las notificaciones recibidas en virtud del presente artículo, garantizando al mismo tiempo la confidencialidad y la protección adecuada de la información facilitada por la entidad notificante. Sin perjuicio de la prevención, 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.

CAPITULO VII

**SUPERVISIÓN Y EJECUCIÓN**

*Artículo 31*

**Aspectos generales relativos a la supervisión y la ejecución**

1. Los Estados miembros velarán por que sus autoridades competentes supervisen efectivamente y adopten las medidas necesarias para garantizar el cumplimiento de la presente Directiva.

2. Los Estados miembros podrán permitir que sus autoridades competentes den prioridad a sus funciones de supervisión. Dicha prioridad se fundamentará en un enfoque basado en el riesgo. A tal efecto, cuando lleven a cabo sus funciones de supervisión previstas en los artículos 32 y 33, las autoridades competentes podrán establecer metodologías de supervisión que permitan priorizar dichas funciones aplicando un enfoque basado en el riesgo.

3. Las autoridades competentes cooperarán estrechamente con las autoridades de control con arreglo al Reglamento (UE) 2016/679 cuando hagan frente a incidentes que den lugar a violaciones de la seguridad de los datos personales, sin perjuicio de las competencias y funciones de las autoridades de control con arreglo a dicho Reglamento.

4. 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 imposición de medidas de ejecución con respecto al incumplimiento de la presente Directiva, las autoridades competentes dispongan de las competencias adecuadas para llevar a cabo dichas funciones con independencia operativa con respecto a las entidades de la Administración pública 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 legislativos e institucionales nacionales.

*Artículo 32*

**Medidas de supervisión y ejecución relativas a entidades esenciales**

1. Los Estados miembros garantizarán que las medidas de supervisión o ejecución impuestas a las entidades esenciales en relación con las obligaciones establecidas 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, dispongan de competencias para someter a dichas entidades a, como mínimo:

a) inspecciones *in situ* y supervisión a distancia, incluidos controles aleatorios realizados por profesionales cualificados;

b) auditorías de seguridad periódicas y específicas llevadas a cabo por un organismo independiente o una autoridad competente;

c) auditorías ad hoc, en particular cuando así lo justifiquen un incidente significativo o un incumplimiento de la presente Directiva por parte de la entidad esencial;

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

e) solicitudes de información necesaria para evaluar las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de presentar información a las autoridades competentes con arreglo al artículo 27;

f) solicitudes de acceso a datos, documentos e 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.

Las auditorías de seguridad específicas a que se refiere el párrafo primero, letra b), se basarán en evaluaciones del riesgo realizadas por la autoridad competente o la entidad auditada, o en otra información disponible relacionada con el riesgo.

Los resultados de cualquier auditoría de seguridad específica se pondrán a disposición de la autoridad competente. Los costes de dicha auditoría de seguridad específica realizada por un organismo independiente serán sufragados por la entidad auditada, salvo en aquellos casos debidamente motivados en los que la autoridad competente decida lo contrario.

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

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

a) apercibir por incumplimientos de la presente Directiva por parte de las entidades afectadas;

b) adoptar instrucciones vinculantes, en particular sobre las medidas necesarias para prevenir o subsanar un incidente, así como plazos para la ejecución de esas medidas y notificar su aplicación, o una orden de requerimiento para que las entidades afectadas subsanen las deficiencias detectadas o los incumplimientos de la presente Directiva;

c) exigir a las entidades afectadas que pongan fin a las conductas que infringen la presente Directiva y que se abstengan de repetirlas;

d) exigir a las entidades afectadas que garanticen que sus medidas para la gestión de riesgos de ciberseguridad son conformes con lo dispuesto en el artículo 21 o que cumplan las obligaciones de notificación establecidas en el artículo 23 de una manera específica y en un plazo concreto;

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

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

g) designar un responsable de supervisión con funciones claramente definidas para que supervise, durante un período determinado, el cumplimiento por parte de las entidades afectadas de las obligaciones previstas en los artículos 21 y 23;

h) ordenar a las entidades afectadas que hagan públicos determinados aspectos del incumplimiento de la presente Directiva de una manera específica;

i) imponer o solicitar la imposición por parte de los organismos u órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 34 a título adicional respecto de cualquiera de las medidas referidas en las letras a) a h) del presente apartado.

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 sus 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 temporalmente o solicitar a un organismo de certificación o autorización o a un órgano jurisdiccional, de conformidad con el Derecho nacional, que suspenda temporalmente una certificación o autorización referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por la entidad esencial;

b) solicitar que los organismos o los órganos jurisdiccionales competentes de acuerdo con el Derecho nacional prohíban temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o representante legal en dicha entidad esencial ejercer funciones de dirección en dicha entidad.

Las suspensiones o las prohibiciones temporales impuestas en virtud del presente apartado se aplicarán únicamente hasta que la entidad afectada adopte las medidas necesarias para subsanar las deficiencias o cumplir los requisitos de la autoridad competente a instancias de la cual se aplicaron dichas medidas de ejecución. La imposición de tales suspensiones o prohibiciones temporales estará sujeta a las garantías procesales adecuadas conforme a los principios generales del Derecho de la Unión y de la Carta, incluido el derecho a la tutela judicial efectiva y a un juicio justo, la presunción de inocencia y los derechos de la defensa.

Las medidas de ejecución previstas en el presente apartado no serán 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 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 la presente Directiva.

Por lo que respecta a las entidades de la Administración pública, el presente apartado se entenderá sin perjuicio del Derecho nacional en materia de responsabilidad de los funcionarios y de los cargos electos o designados.

7. Cuando se adopte una medida de ejecución contemplada en el apartado 4 o 5, las autoridades competentes respetarán los derechos de la defensa y tendrán en cuenta las circunstancias de cada caso particular y, como mínimo, los siguientes aspectos:

a) la gravedad del incumplimiento y la importancia de las disposiciones infringidas, entre otros, constituyen en todo caso incumplimientos graves:

   i) los incumplimientos reiterados;

   ii) la ausencia de notificación o subsanación de los incidentes significativos,

   iii) la ausencia de subsanación de deficiencias tras recibir instrucciones vinculantes de las autoridades competentes;

   iv) la obstrucción de las auditorías o actividades de control ordenadas por la autoridad competente tras la constatación de un incumplimiento;

   v) el suministro de información falsa o manifiestamente imprecisa en relación con las medidas de gestión del riesgo de ciberseguridad o las obligaciones de notificación establecidas en los artículos 21 y 23;

b) la duración del incumplimiento;

c) todo incumplimiento anterior relevante cometido por la entidad afectada;

d) todo perjuicio material o inmaterial causado, incluidas las pérdidas financieras o económicas, los efectos para otros servicios y el número de usuarios afectados;

e) cualquier intencionalidad o negligencia por parte del autor del incumplimiento;

f) cualesquiera medidas adoptadas por la entidad para prevenir o reducir los perjuicios materiales o inmateriales;

g) cualquier adhesión a códigos de conducta o a mecanismos de certificación aprobados;

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

8. Las autoridades competentes argumentarán detalladamente sus medidas de ejecución. Antes de adoptar tales medidas, las autoridades competentes notificarán a las entidades afectadas sus constataciones preliminares. También concederán a dichas entidades un plazo razonable para formular observaciones, salvo en casos debidamente motivados en los que, de otro modo, se obstaculizaría la actuación inmediata para prevenir incidentes o responder a ellos.

9. Los Estados miembros velarán por que sus autoridades competentes designadas con arreglo a la presente Directiva informen a las autoridades competentes pertinentes del mismo Estado miembro designadas con arreglo a la Directiva (UE) 2022/2557 cuando ejerzan sus facultades de supervisión y ejecución con objeto de garantizar el cumplimiento de la presente Directiva por parte de una entidad identificada como crítica con arreglo a la Directiva (UE) 2022/2557. Cuando proceda, las autoridades competentes designadas con arreglo a la Directiva (UE) 2022/2557 podrán solicitar a las autoridades competentes designadas con arreglo a la presente Directiva que ejerzan sus facultades de supervisión y ejecución respecto a una entidad que esté identificada como entidad crítica con arreglo a la Directiva (UE) 2022/2557.

10. Los Estados miembros velarán por que sus autoridades competentes con arreglo a la presente Directiva cooperen con las autoridades competentes pertinentes del Estado miembro en cuestión designadas con arreglo al Reglamento (UE) 2022/2554 En particular, los Estados miembros velarán por que sus autoridades competentes designadas con arreglo a la presente Directiva informen al Foro de Supervisión creado en virtud del artículo 32, apartado 1, del Reglamento (UE) 2022/2554 cuando ejerzan sus facultades de supervisión y ejecución al objeto de garantizar el cumplimiento por parte de una entidad esencial que sea designada como proveedor tercero esencial de servicios de TIC en virtud del artículo 31 del Reglamento (UE) 2022/2554 de la presente Directiva.

*Artículo 33*

**edidas de supervisión y ejecución en relación con entidades importantes**

1. Cuando dispongan de pruebas, indicios o información de que una entidad importante presuntamente no cumple la presente Directiva, en particular sus artículos 21 y 23, los Estados miembros garantizarán que las autoridades competentes actúen, cuando proceda, a través de medidas de supervisión *a posteriori*. Los Estados miembros velarán por que esas medidas sean eficaces, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso.

2. Los Estados miembros velarán por que las autoridades competentes, cuando ejerzan sus funciones de supervisión en relación con entidades importantes, dispongan de competencias para someter a dichas entidades a, como mínimo:

a) inspecciones *in situ* y supervisión *a posteriori* a distancia a cargo de profesionales cualificados;

b) auditorías de seguridad específicas que efectuará un organismo independiente o una autoridad competente;

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

d) solicitudes de información necesaria para evaluar *a posteriori* las medidas para la gestión de riesgos de ciberseguridad adoptadas por la entidad afectada, en particular las políticas de ciberseguridad documentadas, así como el cumplimiento de la obligación de presentar información a las autoridades competentes en virtud del artículo 27;

e) solicitudes de acceso a datos, documentos o información necesaria para llevar a cabo sus funciones de supervisión;

f) 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.

Las auditorías de seguridad específicas a que se refiere el párrafo primero, letra b), se basarán en evaluaciones del riesgo realizadas por la autoridad competente o la entidad auditada, o en otra información disponible relacionada con el riesgo.

Los resultados de cualquier auditoría de seguridad específica se pondrán a disposición de la autoridad competente. Los costes de dicha auditoría de seguridad específica realizada por un organismo independiente serán sufragados por la entidad auditada, salvo en aquellos casos debidamente motivados en los que la autoridad competente decida lo contrario.

3. En el ejercicio de sus competencias con arreglo al apartado 2, letras d), e) o f), 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 para, como mínimo:

a) apercibir por el incumplimiento de la presente Directiva a las entidades afectadas;

b) adoptar instrucciones vinculantes o una orden de requerimiento para que las entidades afectadas subsanen las deficiencias detectadas o los incumplimientos de en la presente Directiva;

c) ordenar a las entidades afectadas que pongan fin a las conductas que infrinjan la presente Directiva y que se abstengan de repetirlas;

d) ordenar a las entidades afectadas que garanticen que sus medidas para la gestión de riesgos de ciberseguridad son conformes con lo dispuesto en el artículo 21 o que cumplan las obligaciones de notificación establecidas en el artículo 23 de una manera específica y en un plazo concreto;

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

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

g) ordenar a las entidades afectadas que hagan públicos determinados aspectos del incumplimiento de la presente Directiva de una manera específica;

h) imponer o solicitar la imposición por parte de los organismos u órganos jurisdiccionales competentes de acuerdo con la legislación nacional de una multa administrativa de conformidad con el artículo 34 a título adicional respecto de cualquiera de las medidas referidas en las letras a) a g) del presente apartado.

5. El artículo 32, apartados 6, 7 y 8, se aplicará *mutatis mutandis* a las medidas de supervisión y ejecución previstas en el presente artículo en el caso de las entidades importantes.

6. Los Estados miembros velarán por que sus autoridades competentes con arreglo a la presente Directiva cooperen con las autoridades competentes pertinentes del Estado miembro en cuestión designadas con arreglo al Reglamento (UE) 2022/2554 En particular, los Estados miembros velarán por que sus autoridades competentes designadas con arreglo a la presente Directiva informen al Foro de Supervisión creado en virtud del artículo 32, apartado 1, del Reglamento (UE) 2022/2554 cuando ejerzan sus facultades de supervisión y ejecución al objeto de garantizar el cumplimiento por parte de una entidad importante que sea designada como proveedor tercero esencial de servicios de TIC en virtud del artículo 31 del Reglamento (UE) 2022/2554 de la presente Directiva.

*Artículo 34*

**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 incumplimientos de la presente Directiva sean efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso individual.

2. Las multas administrativas se impondrán a título adicional respecto a cualquiera de las medidas contempladas en el artículo 32, apartado 4, letras a) a h), el artículo 32, apartado 5, y el artículo 33, apartado 4, letras a) a g).

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 previstos en el artículo 32, apartado 7.

4. Los Estados miembros garantizarán que las entidades esenciales sean sancionadas por el incumplimiento de los artículos 21 o 23, de conformidad con los apartados 2 y 3 del presente artículo, con multas administrativas de un máximo de, al menos, 10 000 000 EUR o de un máximo de, al menos, 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.

5. Los Estados miembros garantizarán que las entidades importantes sean sancionadas por el incumplimiento de los artículos 21 o 23, de acuerdo con los apartados 2 y 3 del presente artículo, con multas administrativas de un máximo de, al menos, 7 000 000 EUR o de un máximo de, al menos, el 1,4 % 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.

6. Los Estados miembros podrán prever la facultad de imponer multas coercitivas para obligar a una entidad esencial o importante a poner fin a un incumplimiento de la presente Directiva de conformidad con una decisión previa de la autoridad competente.

7. Sin perjuicio de las facultades de las autoridades competentes conferidas en virtud de los artículos 32 y 33, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a las entidades de la Administración pública.

8. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, ese Estado miembro velará por que el presente artículo se aplique 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 acción 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. El Estado miembro notificará la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 17 de octubre de 2024, y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

*Artículo 35*

**Incumplimientos que conllevan una violación de la seguridad de los datos personales**

1. Cuando las autoridades competentes tengan constancia en el transcurso de ejercicio de sus funciones de supervisión o ejecución de que el incumplimiento de las obligaciones establecidas en los artículos 21 y 23 de la presente Directiva por parte una entidad esencial o importante puede 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 demora indebida a las autoridades de control a que se refieren los artículos 55 y 56 de dicho Reglamento.

2. Cuando las autoridades de control a que se refieren los artículos 55 o 56 del Reglamento (UE) 2016/679 impongan una multa administrativa en virtud del artículo 58, apartado 2, letra i), de dicho Reglamento, las autoridades competentes no impondrán una multa administrativa en virtud del artículo 34 de la presente Directiva por un incumplimiento contemplado en el apartado 1 del presente artículo derivado de la misma conducta que fue objeto de la multa administrativa con arreglo al artículo 58, apartado 2, letra i), del Reglamento (UE) 2016/679. Las autoridades competentes podrán, no obstante, imponer las medidas de ejecución previstas en el artículo 32, apartado 4, letras a) a h), el artículo 32, apartado 5, y el artículo 33, apartado 4, letras a) a g), 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 informará a la autoridad de control establecida en su propio Estado miembro de la posible violación de la seguridad de los datos personales a que se refiere el apartado 1.

*Artículo 36*

**Sanciones**

Los Estados miembros establecerán el régimen de sanciones aplicables a cualquier incumplimiento 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. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, a más tardar el 17 de enero de 2025, y le notificarán sin demora toda modificación posterior.

*Artículo 37*

**Asistencia mutua**

1. Cuando una entidad preste servicios en más de un Estado miembro, o preste servicios en uno o varios Estados miembros y sus sistemas de redes y de información estén situados en otro u otros Estados miembros, las autoridades competentes de los Estados miembros 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 medidas de supervisión o ejecución;

c) que una autoridad competente, al recibir una solicitud motivada de otra autoridad competente, preste a la otra autoridad competente asistencia mutua proporcionada a los recursos de los que dispone para que las medidas de supervisión o ejecución puedan aplicarse de manera efectiva, eficiente y coherente.

La asistencia mutua contemplada en el párrafo primero, letra c), 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 se determine que la autoridad carece de competencias para prestar la asistencia requerida, o que dicha asistencia no se adecúa a las funciones de supervisión de la autoridad competente, o que la solicitud se refiere a información o implica actividades que, de revelarse o llevarse a cabo, resultaría contraría a intereses esenciales de la seguridad nacional, la seguridad pública o la defensa de dicho Estado miembro. Antes de denegar dicha solicitud, la autoridad competente consultará a las demás autoridades competentes afectadas, así como, a petición de uno de los Estados miembros afectados, a la Comisión y a la ENISA.

2. Cuando proceda y de común acuerdo, las autoridades competentes de varios Estados miembros podrán emprender medidas conjuntas de supervisión.

CAPÍTULO VIII

**ACTOS DELEGADOS Y DE EJECUCIÓN**

*Artículo 38*

**Ejercicio de la delegación**

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar actos delegados mencionados en el artículo 24, apartado 2, se otorgan a la Comisión por un período de cinco años a partir del 16 de enero de 2023.

3. La delegación de poderes mencionada en el artículo 24, apartado 2, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 24, apartado 2, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

*Artículo 39*

**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.

CAPÍTULO IX

**DISPOSICIONES FINALES**

*Artículo 40*

**Revisión**

A más tardar el 17 de octubre de 2027 y posteriormente cada 36 meses, la Comisión revisará el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. En concreto, el informe evaluará la importancia de la magnitud de las entidades afectadas, los sectores, los subsectores 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 tal fin y con vistas a ampliar la cooperación estratégica y operativa, la Comisión tendrá en cuenta los informes del Grupo de Cooperación y de la red de CSIRT sobre la experiencia adquirida a nivel estratégico y operativo. El informe irá acompañado, cuando sea necesario, de una propuesta legislativa.

*Artículo 41*

**Transposición**

1. A más tardar el 17 de octubre de 2024, los Estados miembros adoptarán y publicarán las medidas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

Aplicarán dichas disposiciones a partir del 18 de octubre de 2024.

2. Cuando los Estados miembros adopten las disposiciones a que se refiere el apartado 1, 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 42*

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

Se suprime el artículo 19 del Reglamento (UE) n.º 910/2014 con efectos a partir del 18 de octubre de 2024.

*Artículo 43*

**Modificación de la Directiva (UE) 2018/1972**

Se suprimen los artículos 40 y 41 Directiva (UE) 2018/1972 con efectos a partir del 18 de octubre de 2024.

*Artículo 44*

**Derogación**

Queda derogada la Directiva (UE) 2016/1148 con efectos a partir del 18 de octubre de 2024.

Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva con arreglo a la tabla de correspondencias que figura en el anexo III.

*Artículo 45*

**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 46*

**Destinatarios**

Los destinatarios de la presente Directiva son los Estados miembros.

Hecho en Estrasburgo, el 14 de diciembre de 2022.

| | |
|---|---|
| *Por el Parlamento Europeo* | *Por el Consejo* |
| *La Presidenta* | *El Presidente* |
| R. METSOLA | M. BEK |

*ANEXO I*

**SECTORES DE ALTA CRITICIDAD**

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 1. Energía | a) Electricidad | — Empresas eléctricas, tal como se definen en el artículo 2, punto 57, de la Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo ([1]), que efectúan la función de «suministro», tal como se define en el artículo 2, punto 12, de dicha Directiva |
| | | — Gestores de la red de distribución, tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944 |
| | | — Gestores de la red de transporte, tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944 |
| | | — Productores, tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944 |
| | | — Operadores designados para el mercado eléctrico, tal como se definen en el artículo 2, punto 8, del Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo ([2])<br>— Participantes en el mercado de la electricidad, tal como se definen en 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 define en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944<br>— Operadores de un punto de recarga que sean responsable de la gestión y explotación de un punto de recarga, que presta un servicio de recarga al usuario final también en nombre y por cuenta de un proveedor de servicios de movilidad |
| | b) Sistemas urbanos de calefacción y de refrigeración | — Operadores de sistemas urbanos de calefacción o de refrigeración, tal como se definen en el artículo 2, punto 19, de la Directiva (UE) 2018/2001 del Parlamento Europeo y del Consejo ([3]) |
| | c) Crudo | — Operadores de oleoductos de transporte de crudo |
| | | — Operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte |
| | | — Entidades centrales de almacenamiento, tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo ([4]) |
| | d) Gas | — Empresas suministradoras de gas, tal como se definen en el artículo 2, punto 8, de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo ([5]) |
| | | — Gestores de la red de distribución, tal como se definen en el artículo 2, punto 6, de la Directiva 2009/73/CE |
| | | — Gestores de la red de transporte, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2009/73/CE |
| | | — Gestores de almacenamientos, tal como se definen en el artículo 2, punto 10, de la Directiva 2009/73/CE |
| | | — Gestores de la red de GNL, tal como se definen en el artículo 2, punto 12, de la Directiva 2009/73/CE |
| | | — Compañías de gas natural, tal como se definen en 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 |

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 2. Transporte | a) Transporte aéreo | — Compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008 utilizadas con fines comerciales |
| | | — Entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo ([6]); aeropuertos, tal como se definen en 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 del Parlamento Europeo y del Consejo ([7]); y 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, tal como se definen en el artículo 2, punto 1, del Reglamento (CE) n.º 549/2004 del Parlamento Europeo y del Consejo ([8]) |
| | b) Transporte por ferrocarril | — Administradores de infraestructuras, tal como se definen en el artículo 3, punto 2, de la Directiva 2012/34/UE del Parlamento Europeo y del Consejo ([9]) |
| | | — Empresas ferroviarias, tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, incluidos los explotadores de instalaciones de servicio, tal como se definen en el artículo 3, punto 12 de dicha Directiva |
| | c) Transporte marítimo y fluvial | — Empresas de transporte marítimo, fluvial y de cabotaje, tanto de pasajeros como de mercancías, tal como se definen para el transporte marítimo en el anexo I del Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo ([10]), sin incluir los buques particulares explotados por esas empresas |
| | | — Organismos gestores de los puertos, tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE del Parlamento Europeo y del Consejo ([11]), incluidas sus instalaciones portuarias, tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.º 725/2004, y entidades que operan obras y equipos que se encuentran en los puertos |
| | | — Operadores de servicios de tráfico de buques (STB), tal como se definen en el artículo 3, letra o), de la Directiva 2002/59/CE del Parlamento Europeo y del Consejo ([12]) |
| | d) Transporte por carretera | — Autoridades viarias, tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión ([13]) responsables del control de la gestión del tráfico, excluidas las entidades públicas para las cuales la gestión del tráfico o la explotación de sistemas de transporte inteligentes sea una parte no esencial de su actividad general |
| | | — Operadores de sistemas de transporte inteligentes, tal como se definen en el artículo 4, punto 1, de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo ([14]) |
| 3. Banca | | Entidades de crédito, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([15]) |
| 4. Infraestructuras de los mercados financieros | | — Gestores de centros de negociación, tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo ([16]) |
| | | — Entidades de contrapartida central (ECC), tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo ([17]) |

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 5. Sector sanitario | | — Prestadores de asistencia sanitaria, tal como se definen en el artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo ([18]) |
| | | — Laboratorios de referencia de la UE, tal como se definen en el artículo 15, del Reglamento (UE) .../...del Parlamento Europeo y del Consejo ([19]) |
| | | — Entidades que realizan actividades de investigación y desarrollo de medicamentos, tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo ([20])<br>— Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2<br>— Entidades que fabrican productos sanitarios que se consideran esenciales en situaciones de emergencia de salud pública («lista de productos sanitarios esenciales durante la emergencia de salud pública») en el sentido del artículo 22 del Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo ([21]) |
| 6. Agua potable | | Suministradores y distribuidores de aguas destinadas al consumo humano, tal como se definen en el artículo 2, punto 1, letra a), de la Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo ([22]), excluidos los distribuidores para los que la distribución de aguas destinadas al consumo humano sea una parte no esencial de su actividad general de distribución de otros bienes y productos básicos |
| 7. Aguas residuales | | Empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, tal como se definen en el artículo 2, puntos 1 a 3, de la Directiva 91/271/CEE del Consejo ([23]), excluidas las empresas para las que la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales sea una parte no esencial de su actividad general |
| 8. Infraestructura digital | | — Proveedores de puntos de intercambio de internet |
| | | — Proveedores de servicios de DNS, excluidos los operadores de servidores raíz |
| | | — Registros de nombres de dominio de primer nivel |
| | | — Proveedores de servicios de computación en nube |
| | | — Proveedores de servicios de centro de datos |
| | | — Proveedores de redes de distribución de contenidos |
| | | — Prestadores de servicios de confianza |
| | | — Proveedores de redes públicas de comunicaciones electrónicas |
| | | — Proveedores de servicios de comunicaciones electrónicas disponibles para el público |
| 9. Gestión de servicios de TIC (de empresa a empresa) | | — Proveedores de servicios gestionados<br>— Proveedores de servicios de seguridad gestionados |

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 10. Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales | | — Entidades de la Administración pública central, tal como se definen en el Estado miembro con arreglo a las disposiciones del Derecho nacional<br>— Entidades de la Administración pública a escala regional, según su definición en el Estado miembro con arreglo a las disposiciones del Derecho nacional |
| 11. 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 |

([1]) 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).
([2]) 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).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) 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).
([7]) 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).
([8]) 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).
([9]) 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).
([10]) 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).
([11]) 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).
([12]) 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).
([13]) 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).
([14]) 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).
([15]) 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 por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).
([16]) 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).
([17]) 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).
([18]) 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).

([19]) Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo, de 23 de noviembre de 2022, sobre las amenazas transfronterizas graves para la salud y por el que se deroga la Decisión n.º 1082/2013/UE (DO L 314 de 6.12.2022, p. 26).

([20]) 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).

([21]) Reglamento (UE) 2022/123 del Parlamento Europeo y del Consejo, de 25 de enero de 2022, 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 (DO L 20 de 31.1.2022, p. 1).

([22]) Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2020, relativa a la calidad de las aguas destinadas al consumo humano (DO L 435 de 23.12.2020, p. 1).

([23]) 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).

*ANEXO II*

**OTROS SECTORES CRÍTICOS**

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 1. Servicios postales y de mensajería | | Proveedores de servicios postales, tal como se definen en el artículo 2, punto 1 *bis*, de la Directiva 97/67/CE, incluidos los proveedores de servicios de mensajería |
| 2. Gestión de residuos | | Empresas que realizan la gestión de residuos, tal como se definen en el artículo 3, punto 9, de la Directiva 2008/98/CE del Parlamento Europeo y del Consejo ([1]), excepto aquellas para las que la gestión de residuos no es su principal actividad económica |
| 3. Fabricación, producción y distribución de sustancias y mezclas químicas | | Empresas que realizan la fabricación de sustancias y la distribución de sustancias o mezclas, tal como se definen en el artículo 3, puntos 9 y 14, del Reglamento (CE) n.º 1907/2006 del Parlamento Europeo y del Consejo ([2]) y empresas que realizan la producción de artículos, tal como se definen en el artículo 3, punto 3, de dicho Reglamento, a partir de sustancias y mezclas |
| 4. Producción, transformación y distribución de alimentos | | Empresas alimentarias, tal como se definen en el artículo 3, punto 2, del Reglamento (CE) n.º 178/2002 del Parlamento Europeo y del Consejo ([3]), que se dediquen a la distribución al por mayor y a la producción y transformación industriales |
| 5. Fabricación | a) Fabricación de productos sanitarios y productos sanitarios para diagnóstico *in vitro* | Entidades que fabrican los productos sanitarios, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo ([4]), y entidades que fabrican los productos sanitarios para diagnóstico *in vitro*, tal como se definen en el artículo 2, punto 2, del Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo ([5]), excepto las entidades que fabrican productos sanitarios a que se refiere el anexo I, punto 5, quinto guion, de la presente Directiva |
| | b) Fabricación de productos informáticos, electrónicos y ópticos | 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 | 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. | 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 | 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 | Empresas que realizan cualquiera de las actividades económicas a que se refiere la sección C, división 30, de la NACE Rev. 2 |

| Sector | Subsector | Tipo de entidad |
|---|---|---|
| 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 |
| 7. Investigación | | Organismos de investigación |

([1]) 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).

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

*ANEXO III*

**TABLA DE CORRESPONDENCIAS**

| Directiva (UE) 2016/1148 | Presente Directiva |
|---|---|
| Artículo 1, apartado 1 | Artículo 1, apartado 1 |
| Artículo 1, apartado 2 | Artículo 1, apartado 2 |
| Artículo 1, apartado 3 | – |
| Artículo 1, apartado 4 | Artículo 2, apartado 12 |
| Artículo 1, apartado 5 | Artículo 2, apartado 13 |
| Artículo 1, apartado 6 | Artículo 2, apartados 6 y 11 |
| Artículo 1, apartado 7 | Artículo 4 |
| Artículo 2 | Artículo 2, apartado 14 |
| Artículo 3 | Artículo 5 |
| Artículo 4 | Artículo 6 |
| Artículo 5 | – |
| Artículo 6 | – |
| Artículo 7, apartado 1 | Artículo 7, apartados 1 y 2 |
| Artículo 7, apartado 2 | Artículo 7, apartado 4 |
| Artículo 7, apartado 3 | Artículo 7, apartado 3 |
| Artículo 8, apartados 1 a 5 | Artículo 8, apartados 1 a 5 |
| Artículo 8, apartado 6 | Artículo 13, apartado 4 |
| Artículo 8, apartado 7 | Artículo 8, apartado 6 |
| Artículo 9, apartados 1, 2 y 3 | Artículo 10, apartados 1, 2 y 3 |
| Artículo 9, apartado 4 | Artículo 10, apartado 9 |
| Artículo 9, apartado 5 | Artículo 10, apartado 10 |
| Artículo 10, apartados 1, 2 y 3, párrafo primero | Artículo 13, apartados 1, 2 y 3 |
| Artículo 10, apartado 3, párrafo segundo | Artículo 23, apartado 9 |
| Artículo 11, apartado 1 | Artículo 14, apartados 1 y 2 |
| Artículo 11, apartado 2 | Artículo 14, apartado 3 |
| Artículo 11, apartado 3 | Artículo 14, apartado 4, párrafo primero, letras a) a q) y letra s), y apartado 7 |
| Artículo 11, apartado 4 | Artículo 14, apartado 4, párrafo primero, letra r) y párrafo segundo |
| Artículo 11, apartado 5 | Artículo 14, apartado 8 |
| Artículo 12, apartados 1 a 5 | Artículo 15, apartados 1 a 5 |
| Artículo 13 | Artículo 17 |
| Artículo 14, apartados 1 y 2 | Artículo 21, apartados 1 a 4 |
| Artículo 14, apartado 3 | Artículo 23, apartado 1 |
| Artículo 14, apartado 4 | Artículo 23, apartado 3 |
| Artículo 14, apartado 5 | Artículo 23, apartados 5, 6 y 8 |

| Directiva (UE) 2016/1148 | Presente Directiva |
|---|---|
| Artículo 14, apartado 6 | Artículo 23, apartado 7 |
| Artículo 14, apartado 7 | Artículo 23, apartado 11 |
| Artículo 15, apartado 1 | Artículo 31, apartado 1 |
| Artículo 15, apartado 2, párrafo primero, letra a) | Artículo 32, apartado 2, letra e) |
| Artículo 15, apartado 2, párrafo primero, letra b) | Artículo 32, apartado 2, letra g) |
| Artículo 15, apartado 2, párrafo segundo | Artículo 32, apartado 3 |
| Artículo 15, apartado 3 | Artículo 32, apartado 4, letra b) |
| Artículo 15, apartado 4 | Artículo 31, apartado 3 |
| Artículo 16, apartados 1 y 2 | Artículo 21, apartados 1 a 4 |
| Artículo 16, apartado 3 | Artículo 23, apartado 1 |
| Artículo 16, apartado 4 | Artículo 23, apartado 3 |
| Artículo 16, apartado 5 | – |
| Artículo 16, apartado 6 | Artículo 23, apartado 6 |
| Artículo 16, apartado 7 | Artículo 23, apartado 7 |
| Artículo 16, apartados 8 y 9 | Artículo 21, apartado 5, y Artículo 23, apartado 11 |
| Artículo 16, apartado 10 | – |
| Artículo 16, apartado 11 | Artículo 2, apartados 1, 2, y 3 |
| Artículo 17, apartado 1 | Artículo 33, apartado 1 |
| Artículo 17, apartado 2, letra a) | Artículo 32, apartado 2, letra e) |
| Artículo 17, apartado 2, letra b) | Artículo 32, apartado 4, letra b) |
| Artículo 17, apartado 3 | Artículo 37, apartado 1, letras a) y b) |
| Artículo 18, apartado 1 | Artículo 26, apartado 1, letra b), y apartado 2 |
| Artículo 18, apartado 2 | Artículo 26, apartado 3 |
| Artículo 18, apartado 3 | Artículo 26, apartado 4 |
| Artículo 19 | Artículo 25 |
| Artículo 20 | Artículo 30 |
| Artículo 21 | Artículo 36 |
| Artículo 22 | Artículo 39 |
| Artículo 23 | Artículo 40 |
| Artículo 24 | – |
| Artículo 25 | Artículo 41 |
| Artículo 26 | Artículo 45 |
| Artículo 27 | Artículo 46 |
| Anexo I, punto 1 | Artículo 11, apartado 1 |
| Anexo I, punto 2, letra a), incisos i) a iv) | Artículo 11, apartado 2, letras a) a d) |

| Directiva (UE) 2016/1148 | Presente Directiva |
|---|---|
| Anexo I, punto 2, letra a), inciso v) | Artículo 11, apartado 2, letra f) |
| Anexo I, punto 2, letra b) | Artículo 11, apartado 4 |
| Anexo I, punto 2, letra c), incisos i) y ii) | Artículo 11, apartado 5, letra a) |
| Anexo II | Anexo I |
| Anexo III, puntos 1 y 2 | Anexo II, punto 6 |
| Anexo III, punto 3 | Anexo I, punto 8 |