Diario Oficial de la Unión Europea

L 333

Edición en lengua española

Legislación

65.º año

27 de diciembre de 2022

Sumario

[1] Texto pertinente a efectos del EEE.

ES

Los actos cuyos títulos van impresos en caracteres finos son actos de gestión corriente, adoptados en el marco de la política agraria, y que tienen generalmente un período de validez limitado.

Los actos cuyos títulos van impresos en caracteres gruesos y precedidos de un asterisco son todos los demás actos.

I

(Actos legislativos)

REGLAMENTOS

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

(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]),

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

Considerando lo siguiente:

(1) En la era digital, las tecnologías de la información y la comunicación (TIC) son el soporte de sistemas complejos utilizados en actividades cotidianas. Mantienen nuestras economías en marcha en sectores clave como el sector financiero, y mejoran el funcionamiento del mercado interior. El aumento de la digitalización y la interconexión también amplifica el riesgo relacionado con las TIC, y hace que la sociedad en su conjunto, y el sistema financiero en particular, sea más vulnerable a las ciberamenazas o a las perturbaciones de las TIC. Si bien el uso generalizado de los sistemas de TIC y la alta digitalización y conectividad son hoy en día características fundamentales de las actividades de las entidades financieras de la Unión, sigue siendo necesario abordar e integrar mejor su resiliencia digital en sus marcos operativos más amplios.

(2) El uso de las TIC ha adquirido en las últimas décadas un papel fundamental en la prestación de servicios financieros, hasta el punto de que ahora tiene una importancia fundamental en la ejecución de las funciones cotidianas típicas de todas las entidades financieras. La digitalización abarca ahora, por ejemplo, los pagos, para los que se utilizan, cada vez más, soluciones digitales, en vez de métodos basados en efectivo y papel, así como la compensación y liquidación de valores, la negociación electrónica y algorítmica, las operaciones de préstamo y financiación, la financiación entre particulares, la calificación crediticia, la gestión de siniestros y las operaciones administrativas. El

([1]) DO C 343 de 26.8.2021, p. 1.
([2]) DO C 155 de 30.4.2021, p. 38.
([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.

uso de las TIC también ha transformado el sector de los seguros, desde la aparición de intermediarios de seguros que ofrecen sus servicios en línea y desarrollan su actividad con tecnología aplicada al sector de los seguros (InsurTech) hasta la suscripción de seguros por medios digitales. No solo se ha digitalizado en gran medida todo el sector financiero, sino que la digitalización también ha profundizado las interconexiones y las dependencias tanto dentro del sector financiero como en relación con proveedores terceros de infraestructuras y servicios.

(3) La Junta Europea de Riesgo Sistémico (JERS) reafirmó en un informe de 2020 sobre el ciberriesgo sistémico que el elevado nivel actual de interconexión entre entidades financieras, mercados financieros e infraestructuras de los mercados financieros, y en particular las interdependencias de sus sistemas de TIC, podría constituir una vulnerabilidad sistémica, ya que desde cualquiera de las aproximadamente 22 000 entidades financieras de la Unión podrían propagarse rápidamente a todo el sistema financiero ciberincidentes localizados, sin que los límites geográficos supongan un obstáculo. Las vulneraciones graves relacionadas con las TIC que tienen lugar en el sector financiero no afectan únicamente a las entidades financieras de forma aislada. También allanan el camino para la propagación de vulnerabilidades localizadas a través de los canales de transmisión financieros y pueden provocar consecuencias negativas para la estabilidad del sistema financiero de la Unión, por ejemplo, fugas de liquidez y una pérdida general de confianza en los mercados financieros.

(4) En los últimos años, los responsables políticos, los reguladores y los organismos de normalización internacionales, de la Unión y nacionales han abordado el riesgo relacionado con las TIC, en un intento de aumentar la resiliencia digital, establecer normas y coordinar el trabajo de regulación o supervisión. A escala internacional, el Comité de Supervisión Bancaria de Basilea, el Comité de Pagos e Infraestructuras del Mercado, el Consejo de Estabilidad Financiera y el Instituto de Estabilidad Financiera, así como el G7 y el G20, procuran proporcionar a las autoridades competentes y a los operadores del mercado de varias jurisdicciones herramientas para reforzar la resiliencia de sus sistemas financieros. Esta labor también se ha visto impulsada por la necesidad de tener debidamente en cuenta el riesgo relacionado con las TIC en el contexto de un sistema financiero mundial altamente interconectado y de tratar de reforzar la coherencia de las mejores prácticas pertinentes.

(5) A pesar de las iniciativas estratégicas y legislativas específicas de la Unión y nacionales, el riesgo relacionado con las TIC sigue representando un desafío para la resiliencia operativa, el rendimiento y la estabilidad del sistema financiero de la Unión. Las reformas que siguieron a la crisis financiera de 2008 reforzaron fundamentalmente la resiliencia financiera del sector financiero de la Unión y tuvieron por objeto salvaguardar la competitividad y la estabilidad de la Unión desde los puntos de vista económico, prudencial y de conducta del mercado. Pese a que la resiliencia digital y la seguridad de las TIC forman parte del riesgo operativo, han recibido menos atención en la agenda normativa posterior a la crisis financiera y se han desarrollado únicamente en algunos ámbitos de la política y el panorama normativo de la Unión en el ámbito de los servicios financieros, o solo en unos pocos Estados miembros.

(6) En su Comunicación de 8 de marzo de 2018 titulada «Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador», la Comisión puso de relieve la importancia capital de hacer que el sector financiero de la Unión sea más resiliente, también desde una perspectiva operativa, para garantizar su seguridad tecnológica y su buen funcionamiento, así como su rápida recuperación de los incidentes y vulneraciones relacionadas con las TIC, lo que permitirá en última instancia que los servicios financieros se presten de manera eficaz y fluida en toda la Unión, también en situaciones de tensión, al tiempo que se preserva la confianza de los consumidores y del mercado.

(7) En abril de 2019, la Autoridad Europea de Supervisión (Autoridad Bancaria Europea, ABE) creada mediante el Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([4]), la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación, AESPJ) creada mediante el Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([5]) y la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados, AEVM) creada mediante el Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del

([4]) Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12).

([5]) Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión (DO L 331 de 15.12.2010, p. 48).

Consejo ([6]) (conocidas colectivamente como «Autoridades Europeas de Supervisión») emitieron conjuntamente dictámenes técnicos en los que pedían un enfoque coherente del riesgo relacionado con las TIC en el ámbito financiero y recomendaban reforzar, de manera proporcionada, la resiliencia operativa digital del sector de los servicios financieros a través de una iniciativa sectorial de la Unión.

(8) El sector financiero de la Unión está regulado por un código normativo único y regido por un sistema europeo de supervisión financiera. No obstante, las disposiciones que abordan la resiliencia operativa digital y la seguridad de las TIC no están todavía plena o coherentemente armonizadas, pese a que la resiliencia operativa digital es vital para garantizar la estabilidad financiera y la integridad del mercado en la era digital y no es menos importante que, por ejemplo, las normas comunes prudenciales o de conducta de mercado. Por consiguiente, deben desarrollarse el código normativo único y el sistema de supervisión para que abarquen también la resiliencia operativa digital, reforzando los mandatos de las autoridades competentes para que puedan supervisar la gestión del riesgo relacionado con las TIC en el sector financiero con el objetivo de proteger la integridad y la eficiencia del mercado interior y facilitar su correcto funcionamiento.

(9) Las disparidades legislativas y unos enfoques de regulación o de supervisión nacionales desiguales por lo que respecta al riesgo relacionado con las TIC generan obstáculos al funcionamiento del mercado interior de los servicios financieros, lo que dificulta el correcto ejercicio de la libertad de establecimiento y la prestación de servicios por parte de las entidades financieras que operan a escala transfronteriza. La competencia entre el mismo tipo de entidades financieras que operan en diferentes Estados miembros también podría verse falseada. Esto sucede, en particular, en ámbitos en los que la armonización a escala de la Unión ha sido muy limitada (como las pruebas de resiliencia operativa digital) o inexistente (como el seguimiento del riesgo de relacionado con las TIC derivado de terceros). Las disparidades derivadas de la evolución prevista a escala nacional podrían generar nuevos obstáculos al funcionamiento del mercado interior en detrimento de los participantes en el mercado y la estabilidad financiera.

(10) Actualmente, dado que las disposiciones sobre el riesgo relacionado con las TIC se han abordado solo parcialmente a escala de la Unión, existen lagunas o solapamientos en ámbitos importantes, como la notificación de incidentes relacionados con las TIC y las pruebas de resiliencia operativa digital, e incoherencias provocadas por la aparición de normas nacionales divergentes o la aplicación ineficaz a efecto de los costes de normas que se solapan. Esto es especialmente perjudicial para quienes hacen un uso intensivo de las TIC, como es el caso del sector financiero, ya que los riesgos tecnológicos no tienen fronteras y el sector financiero ofrece sus servicios a escala ampliamente transfronteriza dentro y fuera de la Unión. Las entidades financieras que operan a escala transfronteriza o que poseen varias autorizaciones (por ejemplo, una misma entidad financiera puede tener una licencia bancaria, una licencia de empresa de servicios de inversión y una licencia de entidad de pago, cada una expedida por una autoridad competente diferente en uno o varios Estados miembros) se enfrentan a retos operativos a la hora de abordar el riesgo relacionado con las TIC y mitigar las repercusiones negativas de los incidentes relacionados con las TIC de manera autónoma, coherente y eficaz en términos de costes.

(11) Dado que el código normativo único no ha ido acompañado de un marco global del riesgo operativo o relacionado con las TIC, es necesaria una mayor armonización de los requisitos clave de resiliencia operativa digital para todas las entidades financieras. El desarrollo de las capacidades en materia de TIC y la resiliencia general por las entidades financieras, sobre la base de estos requisitos clave, con vistas a hacer frente a las interrupciones operativas, contribuiría a preservar la estabilidad e integridad de los mercados financieros de la Unión y, de este modo, a garantizar un elevado nivel de protección de los inversores y consumidores de la Unión. Puesto que el objetivo del presente Reglamento es contribuir al buen funcionamiento del mercado interior, debe basarse en las disposiciones del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), interpretadas de conformidad con la jurisprudencia reiterada del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia»).

(12) El presente Reglamento tiene por objeto consolidar y actualizar los requisitos relativos al riesgo relacionado con las TIC como parte de los requisitos en materia de riesgo operativo que se han abordado hasta la fecha por separado en distintos actos jurídicos de la Unión. Si bien esos actos abarcaron las principales categorías de riesgo financiero (por ejemplo, riesgo de crédito, riesgo de mercado, riesgo de crédito de contraparte y riesgo de liquidez, riesgo de conducta de mercado), no abordaron de manera global, en el momento de su adopción, todos los componentes de la resiliencia operativa. Las normas en materia de riesgo operativo, cuando se desarrollaron más en estos actos jurídicos de la Unión, a menudo se decantaron por un enfoque cuantitativo tradicional para abordar el riesgo (a saber, establecer un requisito de capital para cubrir el riesgo relacionado con las TIC) en vez de por normas

([6]) Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión (DO L 331 de 15.12.2010, p. 84).

cualitativas específicas con respecto a las capacidades de protección, detección, contención, recuperación y reparación frente a incidentes relacionados con las TIC o en lo relativo a las capacidades de notificación y relativas a las pruebas digitales. El objetivo principal de dichos actos era recoger y actualizar normas esenciales sobre supervisión prudencial, integridad del mercado o conducta. La consolidación y la actualización de las distintas normas sobre el riesgo relacionado con las TIC deben permitir reunir por primera vez de manera coherente en un único acto legislativo todas las disposiciones que abordan el riesgo digital en el sector financiero. Así pues, el presente Reglamento colma las lagunas o subsana las incoherencias de algunos de los actos jurídicos anteriores, también en relación con la terminología utilizada en ellos, y hace referencia explícita al riesgo relacionado con las TIC a través de normas específicas sobre las capacidades de gestión de este riesgo, la notificación de incidentes, las pruebas de resiliencia operativa y el seguimiento del riesgo relacionado con las TIC derivado de terceros. Por consiguiente, el presente Reglamento debe también sensibilizar respecto al riesgo relacionado con las TIC y reconocer que los incidentes relacionados con las TIC y la falta de resiliencia operativa pueden poner en peligro la solidez de las entidades financieras.

(13) Las entidades financieras deben seguir el mismo enfoque y las mismas normas basadas en principios a la hora de abordar el riesgo relacionado con las TIC teniendo en cuenta su tamaño y su perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones. La coherencia contribuye a aumentar la confianza en el sistema financiero y a preservar su estabilidad, especialmente en tiempos de elevada dependencia de los sistemas, plataformas e infraestructuras de TIC, que conlleva un mayor riesgo digital. El respeto de una ciberhigiene básica también debe evitar la imposición de costes elevados a la economía a través de la minimización de las repercusiones y los costes de las perturbaciones de las TIC.

(14) Un reglamento contribuye a reducir la complejidad normativa, fomenta la convergencia en materia de supervisión y aumenta la seguridad jurídica y, además, contribuye a limitar los costes de cumplimiento, especialmente para las entidades financieras que operan a escala transfronteriza, y a reducir los falseamientos de la competencia. Por lo tanto, elegir un reglamento para el establecimiento de un marco común para la resiliencia operativa digital de las entidades financieras es la manera más adecuada de garantizar una aplicación homogénea y coherente de todos los componentes de la gestión del riesgo relacionado con las TIC por parte del sector financiero de la Unión.

(15) La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([7]) fue el primer marco horizontal de ciberseguridad establecido a escala de la Unión, y se aplica también a tres tipos de entidades financieras, a saber, las entidades de crédito, los centros de negociación y las entidades de contrapartida central. Sin embargo, dado que la Directiva (UE) 2016/1148 estableció un mecanismo de identificación a escala nacional de los operadores de servicios esenciales, solo determinadas entidades de crédito, centros de negociación y entidades de contrapartida central que han sido identificados por los Estados miembros, han entrado, en la práctica, en su ámbito de aplicación, y se les ha exigido por lo tanto que cumplan los requisitos de notificación de incidentes y seguridad relacionados con las TIC establecidos en dicha Directiva. La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([8]) establece un criterio uniforme para determinar qué entidades entran en su ámbito de aplicación (norma sobre el tamaño máximo), al tiempo que mantiene los tres tipos de entidades financieras en su ámbito de aplicación.

(16) No obstante, dado que el presente Reglamento eleva el nivel de armonización de los distintos componentes de la resiliencia digital mediante la introducción de requisitos en materia de gestión del riesgo relacionado con las TIC y de notificación de incidentes relacionados con las TIC más estrictos que los establecidos en el Derecho vigente de la Unión en materia de servicios financieros, este nivel más elevado constituye una mayor armonización también en comparación con los requisitos establecidos en la Directiva (UE) 2022/2555. Por consiguiente, el presente Reglamento constituye una *lex specialis* con respecto a la Directiva (UE) 2022/2555. Al mismo tiempo, es fundamental mantener una estrecha relación entre el sector financiero y el marco horizontal de ciberseguridad de la Unión tal como se establece actualmente en la Directiva (UE) 2022/2555 para garantizar la coherencia con las estrategias de ciberseguridad adoptadas por los Estados miembros y para permitir que los supervisores financieros tengan conocimiento de los ciberincidentes que afecten a otros sectores cubiertos por dicha Directiva.

([7]) 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).

([8]) 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 se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (véase la página 80 del presente Diario Oficial).

(17) De conformidad con el artículo 4, apartado 2, del Tratado de la Unión Europea, y sin perjuicio del control judicial por parte del Tribunal de Justicia, el presente Reglamento no debe afectar a la responsabilidad de los Estados miembros relativa a las funciones esenciales del Estado que afectan a la seguridad pública, la defensa y la salvaguardia de la seguridad nacional, por ejemplo en casos en los que facilitar información sería contrario a la salvaguardia de la seguridad nacional.

(18) Para permitir el aprendizaje intersectorial y aprovechar eficazmente las experiencias de otros sectores a la hora de hacer frente a las ciberamenazas, las entidades financieras a que se refiere la Directiva (UE) 2022/2555 deben seguir formando parte del «ecosistema» de dicha Directiva [por ejemplo, el Grupo de Cooperación y los equipos de respuesta a incidentes de seguridad informática (CSIRT)]. Las Autoridades Europeas de Supervisión y las autoridades nacionales competentes deben poder participar en los debates estratégicos y en los trabajos técnicos del Grupo de Cooperación con arreglo a dicha Directiva e intercambiar información y seguir cooperando con los puntos de contacto únicos designados o establecidos de conformidad con dicha Directiva. Las autoridades competentes con arreglo al presente Reglamento también deben consultar a los CSIRT y cooperar con ellos. Las autoridades competentes también deben poder solicitar dictámenes técnicos a las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555 y establecer acuerdos de cooperación encaminados a garantizar unos mecanismos de coordinación eficaces y rápidos.

(19) Habida cuenta de las fuertes interrelaciones entre la resiliencia digital y la resiliencia física de las entidades financieras, el presente Reglamento y la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo ([9]) deben adoptar un enfoque coherente por lo que respecta a la resiliencia de las entidades críticas. Dado que las obligaciones de gestión del riesgo relacionado con las TIC y de notificación contempladas en el presente Reglamento abordan de manera global la resiliencia física de las entidades financieras, las obligaciones establecidas en los capítulos III y IV de la Directiva (UE) 2022/2557 no deben aplicarse a las entidades financieras que entran en el ámbito de aplicación de dicha Directiva.

(20) Los proveedores de servicios de computación en nube son una categoría de infraestructura digital cubierta por la Directiva (UE) 2022/2555. El marco de supervisión de la Unión (en lo sucesivo, «marco de supervisión») establecido por el presente Reglamento se aplica a todos los proveedores terceros esenciales de servicios de TIC, incluidos los proveedores de servicios de computación en nube que prestan servicios de TIC a entidades financieras, y debe considerarse complementario de la supervisión en virtud de la Directiva (UE) 2022/2555. Además, en ausencia de un marco horizontal de la Unión que establezca una autoridad de supervisión digital, el marco de supervisión establecido por el presente Reglamento debe abarcar a los proveedores de servicios de computación en nube.

(21) Para mantener el pleno control del riesgo relacionado con las TIC, las entidades financieras necesitan disponer de capacidades globales para permitir una gestión del riesgo relacionado con las TIC sólida y eficaz, así como de mecanismos y políticas específicos para gestionar todos los incidentes relacionados con las TIC y notificar los incidentes graves relacionados con estas. Del mismo modo, las entidades financieras deben contar con políticas para la realización de pruebas de sistemas, controles y procesos relacionados con las TIC, así como para gestionar el riesgo relacionado con las TIC derivado de terceros. Debe elevarse el nivel de referencia en cuanto a la resiliencia operativa digital para las entidades financieras, al tiempo que se permite una aplicación proporcionada de los requisitos para determinadas entidades financieras, en particular las microempresas, así como las entidades financieras sujetas a un marco simplificado de gestión del riesgo relacionado con las TIC. Para facilitar un control eficaz de los fondos de pensiones de empleo que sea proporcionado y responda a la necesidad de reducir las cargas administrativas de las autoridades competentes, las disposiciones nacionales pertinentes en materia de control aplicables a dichas entidades financieras deben tener en cuenta el tamaño y el perfil de riesgo general de estas, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones, también cuando se superen los umbrales pertinentes establecidos en el artículo 5 de la Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo ([10]). En particular, las actividades de control deben centrarse principalmente en la necesidad de abordar los riesgos graves asociados a la gestión del riesgo relacionado con las TIC de una entidad concreta.

([9]) 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 2008/114/CE del Consejo (véase la página 164 del presente Diario Oficial).

([10]) Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2016, relativa a las actividades y la supervisión de los fondos de pensiones de empleo (FPE) (DO L 354 de 23.12.2016, p. 37).

Asimismo, las autoridades competentes deben llevar a cabo de manera atenta pero proporcionada la supervisión de los fondos de pensiones de empleo que, de conformidad con el artículo 31 de la Directiva (UE) 2016/2341, externalizan a proveedores de servicios una parte considerable de su actividad principal, como la gestión de activos, los cálculos actuariales, la contabilidad y la gestión de datos.

(22) Los umbrales de notificación y las taxonomías de incidentes relacionados con las TIC varían considerablemente a escala nacional. Si bien es cierto que se puede alcanzar una base común mediante la labor pertinente emprendida por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) establecida por el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo ([11]) y el Grupo de Cooperación a las que se aplica la Directiva (UE) 2022/2555, para las demás entidades financieras todavía existen, o pueden surgir, enfoques divergentes sobre el establecimiento de los umbrales y el uso de taxonomías. Debido a dichas divergencias, existen múltiples requisitos que deben cumplir las entidades financieras, especialmente cuando operan en varios Estados miembros y cuando forman parte de un grupo financiero. Además, tales divergencias pueden obstaculizar la creación de nuevos mecanismos uniformes o centralizados de la Unión que aceleren el proceso de notificación y apoyen un intercambio rápido y fluido de información entre las autoridades competentes, lo cual es crucial para hacer frente al riesgo relacionado con las TIC en caso de ataques a gran escala con posibles consecuencias sistémicas.

(23) A fin de reducir la carga administrativa y las obligaciones de notificación que podrían constituir una duplicación para determinadas entidades financieras, la obligación de notificar incidentes en virtud de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo ([12]) debe dejar de aplicarse a los proveedores de servicios de pago que entran en el ámbito de aplicación del presente Reglamento. Por consiguiente, las entidades de crédito, las entidades de dinero electrónico, las entidades de pago y los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de dicha Directiva deben notificar a partir de la fecha de aplicación del presente Reglamento, en virtud del presente Reglamento, todos los incidentes operativos o de seguridad relacionados con los pagos que se hayan notificado previamente en virtud de dicha Directiva, con independencia de que dichos incidentes estén o no relacionados con las TIC.

(24) Para que las autoridades competentes puedan desempeñar funciones de control obteniendo una perspectiva completa de la naturaleza, frecuencia, importancia y repercusiones de los incidentes relacionados con las TIC y a fin de mejorar el intercambio de información entre las autoridades públicas pertinentes, incluidas las autoridades policiales y las autoridades de resolución, el presente Reglamento debe establecer un régimen de notificación de incidentes relacionados con las TIC que sea sólido y cuyos requisitos pertinentes colmen las lagunas que actualmente existen en el Derecho en materia de servicios financieros y eliminen los solapamientos y duplicaciones existentes para reducir los costes. Es esencial armonizar el régimen de notificación de incidentes relacionados con las TIC exigiendo a todas las entidades financieras que informen a sus autoridades competentes a través del marco simplificado único que se establece en el presente Reglamento. Además, las Autoridades Europeas de Supervisión deben estar facultadas para especificar en mayor medida los elementos pertinentes para el marco de notificación de incidentes relacionados con las TIC, como la taxonomía, los plazos, los conjuntos de datos, las plantillas y los umbrales aplicables. Para garantizar la plena coherencia con la Directiva (UE) 2022/2555, las entidades financieras deben poder notificar, de manera voluntaria, ciberamenazas importantes a la autoridad competente pertinente cuando consideren que la ciberamenaza es relevante para el sistema financiero, los usuarios del servicio o los clientes.

(25) Los requisitos de las pruebas de resiliencia operativa digital se han desarrollado en determinados subsectores financieros y establecen marcos que no siempre están plenamente armonizados. Esto da lugar a una posible duplicación de costes para las entidades financieras transfronterizas y hace que el reconocimiento mutuo de los resultados de las pruebas de resiliencia operativa digital sea complejo, lo que, a su vez, puede fragmentar el mercado interior.

([11]) 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).

([12]) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35).

(26) Además, cuando no se requieren pruebas de TIC, las vulnerabilidades no se detectan y acaban exponiendo a la entidad financiera al riesgo relacionado con las TIC y, en última instancia, engendran un riesgo mayor para la estabilidad y la integridad del sector financiero. Sin la intervención de la Unión, las pruebas de resiliencia operativa digital seguirían siendo incoherentes y carecerían de un sistema de reconocimiento mutuo de los resultados de las pruebas de TIC en diferentes países y territorios. Asimismo, dado que es poco probable que otros subsectores financieros adopten sistemas de pruebas a una escala significativa, desaprovecharían las ventajas potenciales de un marco de pruebas en cuanto a la revelación de vulnerabilidades y riesgos relacionados con las TIC y la prueba de las capacidades de defensa y la continuidad de la actividad, el cual contribuye a aumentar la confianza de los clientes, los proveedores y los socios comerciales. Para poner remedio a esos solapamientos, divergencias y lagunas, es necesario establecer normas con el fin de coordinar el régimen de pruebas y facilitar así el reconocimiento mutuo de pruebas avanzadas para las entidades financieras que cumplen los criterios establecidos en el presente Reglamento.

(27) La dependencia del uso de servicios de TIC por parte de las entidades financieras se debe en parte a su necesidad de adaptarse a una economía mundial digital competitiva emergente, de aumentar su eficiencia empresarial y de satisfacer la demanda de los consumidores. La naturaleza y el alcance de dicha dependencia han estado en constante evolución en los últimos años, haciendo bajar los costes de la intermediación financiera, permitiendo expandirse a las empresas y ampliar las actividades financieras, y ofreciendo al mismo tiempo una amplia gama de herramientas de TIC para gestionar procesos internos complejos.

(28) Ese amplio uso de los servicios de TIC se pone de manifiesto en acuerdos contractuales complejos, reflejo de las dificultades que a menudo encuentran las entidades financieras a la hora de negociar condiciones contractuales adaptadas a las normas prudenciales u otros requisitos reglamentarios a los que están sujetas, o a la hora de hacer valer derechos específicos, como los derechos de acceso o auditoría, aun cuando estos últimos estén consagrados en sus acuerdos contractuales. Además, muchos de dichos acuerdos contractuales no ofrecen suficientes salvaguardias que permitan el seguimiento completo de los procesos de subcontratación, privando así a la entidad financiera de su capacidad para evaluar los riesgos asociados. Por otra parte, dado que los proveedores terceros de servicios de TIC a menudo prestan servicios estándar a distintos tipos de clientes, tales acuerdos contractuales no siempre satisfacen adecuadamente las necesidades particulares o específicas de los agentes del sector financiero.

(29) Aunque el Derecho de la Unión en materia de servicios financieros contiene determinadas normas generales sobre externalización, el seguimiento de la dimensión contractual no está plenamente establecido en el Derecho de la Unión. A falta de normas claras y específicas de la Unión aplicables a los acuerdos contractuales celebrados con los proveedores terceros de servicios de TIC, no se aborda de manera global la fuente externa de riesgo relacionado con las TIC. Por consiguiente, es necesario establecer determinados principios clave para orientar la gestión por parte de las entidades financieras del riesgo relacionado con las TIC derivado de terceros, que son de especial importancia cuando las entidades financieras recurren a proveedores terceros de servicios de TIC para sustentar funciones esenciales o importantes. Dichos principios deben ir acompañados de un conjunto de derechos contractuales básicos en relación con varios elementos de la ejecución y terminación de acuerdos contractuales, con vistas a ofrecer determinadas salvaguardias mínimas con el fin de reforzar la capacidad de las entidades financieras de hacer efectivamente un seguimiento de todos los riesgos relacionados con las TIC que surjan en el nivel de los proveedores terceros de servicios. Dichos principios son complementarios al Derecho sectorial aplicable a la externalización.

(30) En la actualidad es evidente cierta falta de homogeneidad y convergencia en lo relativo al seguimiento del riesgo relacionado con las TIC derivado de terceros y a las dependencias de terceros en el ámbito de las TIC. A pesar de los esfuerzos para abordar la externalización, como las Directrices sobre externalización de la ABE de 2019 y las Directrices sobre la externalización de servicios a proveedores de servicios en nube de la AEVM de 2021, el Derecho de la Unión no aborda de forma suficiente la cuestión más amplia de contrarrestar el riesgo sistémico que puede desencadenar la exposición del sector financiero a un número limitado de proveedores terceros esenciales de servicios de TIC. La falta de normas a escala de la Unión se ve agravada por la ausencia de normas nacionales sobre mandatos e instrumentos que permitan a los supervisores financieros adquirir una buena comprensión de las dependencias de terceros en el ámbito de las TIC y hacer un seguimiento adecuado de los riesgos derivados de la concentración de las dependencias de terceros en el ámbito de las TIC.

(31) Teniendo en cuenta el posible riesgo sistémico que suponen el aumento de las prácticas de externalización y la concentración de terceros en el sector de las TIC, así como la insuficiencia de los mecanismos nacionales a la hora de ofrecer a los supervisores financieros instrumentos adecuados para cuantificar, calificar y corregir las consecuencias de los riesgos relacionados con las TIC derivados de proveedores terceros esenciales de servicios de TIC, es necesario establecer un marco de supervisión adecuado que permita hacer un seguimiento continuo de las actividades de los proveedores terceros de servicios de TIC que sean esenciales para las entidades financieras, garantizando al mismo tiempo la confidencialidad y seguridad de los clientes que no sean entidades financieras. Si bien la prestación intragrupo de servicios de TIC conlleva riesgos y beneficios específicos, no debe considerarse automáticamente menos arriesgada que la prestación de servicios de TIC por parte de proveedores ajenos a un grupo financiero y debe por lo tanto estar sujeta al mismo marco normativo. Sin embargo, cuando los servicios de TIC se prestan dentro del mismo grupo financiero, las entidades financieras podrían tener un mayor nivel de control sobre los proveedores intragrupo, lo que debería tenerse en cuenta en la evaluación global de riesgos.

(32) Dado que el riesgo relacionado con las TIC es cada vez más y más complejo y sofisticado, la eficacia de las medidas de detección y prevención de dicho riesgo depende en gran medida del intercambio periódico de información sobre amenazas y vulnerabilidades entre las entidades financieras. El intercambio de información contribuye a una mayor concienciación sobre las ciberamenazas. Esto mejora, a su vez, la capacidad de las entidades financieras para evitar que las ciberamenazas se conviertan en incidentes reales relacionados con las TIC y les permite contener de forma más eficaz las repercusiones de tales incidentes y recuperarse con más rapidez. A falta de orientaciones a escala de la Unión, varios factores parecen haber impedido ese intercambio de información, en particular la incertidumbre sobre su compatibilidad con las normas de protección de datos, de defensa de la competencia y de responsabilidad.

(33) Además, las dudas sobre el tipo de información que puede compartirse con otros participantes en el mercado o con autoridades que no son responsables de controlar (como la ENISA, en el caso de la información analítica, o Europol, con fines policiales) hacen que no se comparta información útil. Así pues, en la actualidad, el intercambio de información sigue estando limitado y fragmentado en términos cualitativos y cuantitativos, ya que los intercambios en la materia son principalmente locales (a través de iniciativas nacionales) y no existen acuerdos sistemáticos de intercambio de información a escala de la Unión adaptados a las necesidades de un sistema financiero integrado. Por lo tanto, es importante reforzar esos canales de comunicación.

(34) Debe alentarse a las entidades financieras a intercambiar entre ellas información e inteligencia sobre ciberamenazas y a aprovechar colectivamente sus conocimientos particulares y su experiencia práctica a nivel estratégico, táctico y operativo, con el fin de mejorar sus capacidades para evaluar y hacer un seguimiento de las ciberamenazas, defenderse de ellas y responder a las mismas, todo ello de forma adecuada, participando en acuerdos de intercambio de información. Por lo tanto, es necesario permitir la aparición a escala de la Unión de mecanismos para los acuerdos voluntarios de intercambio de información que, cuando se apliquen en entornos de confianza, ayuden a la comunidad del sector financiero a prevenir las ciberamenazas y responder colectivamente a las mismas limitando rápidamente la propagación del riesgo relacionado con las TIC e impidiendo el posible contagio a través de los canales financieros. Esos mecanismos deben respetar las normas aplicables del Derecho de la competencia de la Unión que se establecen en la Comunicación de la Comisión de 14 de enero de 2011 «Directrices sobre la aplicabilidad del artículo 101 del Tratado de Funcionamiento de la Unión Europea a los acuerdos de cooperación horizontal», así como las normas de la Unión en materia de protección de datos, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([13]). Deben funcionar partiendo del uso de una o varias de las bases jurídicas que se establecen en el artículo 6 de dicho Reglamento, como en el contexto del tratamiento de datos personales que es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, tal como se contempla en su artículo 6, apartado 1, letra f), así como en el contexto del tratamiento de datos personales que es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento o que es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, tal como se contempla en el artículo 6, apartado 1, letras c) y e), respectivamente, de dicho Reglamento.

([13]) 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).

(35) A fin de mantener un elevado nivel de resiliencia operativa digital para todo el sector financiero y, al mismo tiempo, seguir el ritmo de los avances tecnológicos, el presente Reglamento debe abordar los riesgos derivados de todos los tipos de servicios de TIC. A tal fin, la definición de servicios de TIC en el contexto del presente Reglamento debe entenderse de una manera amplia, que abarque los servicios digitales y de datos prestados a través de sistemas de TIC a uno o varios usuarios internos o externos de forma continua. Esa definición debe incluir, por ejemplo, los denominados servicios de transmisión libre, que entran dentro de la categoría de servicios de comunicaciones electrónicas. Debe excluir únicamente la categoría limitada de servicios telefónicos analógicos tradicionales que se clasifican como servicios de red telefónica pública conmutada (RTPC), servicios de línea terrestre, servicios de telefonía convencional (POTS) o servicios de telefonía fija.

(36) No obstante la amplia cobertura prevista en el presente Reglamento, en la aplicación de las normas de resiliencia operativa digital se deben tener en cuenta las importantes diferencias que existen entre entidades financieras por cuanto se refiere a su tamaño y perfil de riesgo general. Como principio general, al distribuir recursos y capacidades para la aplicación del marco de gestión de riesgos relacionados con las TIC, las entidades financieras deben buscar un equilibrio adecuado entre sus necesidades en materia de TIC y su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones, mientras que las autoridades competentes deben seguir evaluando y revisando el enfoque de dicha distribución.

(37) Los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la Directiva (UE) 2015/2366 están explícitamente incluidos en el ámbito de aplicación del presente Reglamento, teniendo en cuenta la naturaleza específica de sus actividades y los riesgos derivados de ellas. Además, las entidades de dinero electrónico y las entidades de pago exentas en virtud del artículo 9, apartado 1, de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo ([14]) y del artículo 32, apartado 1, de la Directiva (UE) 2015/2366 están incluidas en el ámbito de aplicación del presente Reglamento, aunque no hayan recibido autorización de conformidad con la Directiva 2009/110/CE para emitir dinero electrónico, o si no han recibido autorización de conformidad con la Directiva (UE) 2015/2366 para prestar y ejecutar servicios de pago. Sin embargo, las instituciones de giro postal a que se refiere el artículo 2, apartado 5, punto 3, de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo ([15]) quedan excluidas del ámbito de aplicación del presente Reglamento. La autoridad competente de las entidades de pago exentas en virtud de la Directiva (UE) 2015/2366, las entidades de dinero electrónico exentas en virtud de la Directiva 2009/110/CE y los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la Directiva (UE) 2015/2366 debe ser la autoridad competente designada de conformidad con el artículo 22 de la Directiva (UE) 2015/2366.

(38) Dado que las entidades financieras de mayor tamaño podrían disponer de recursos más amplios y movilizar rápidamente fondos para desarrollar estructuras de gobernanza y establecer diversas estrategias empresariales, solo las entidades financieras que no sean microempresas en el sentido del presente Reglamento deben estar obligadas a establecer mecanismos de gobernanza más complejos. Dichas entidades están mejor preparadas, en particular, para establecer funciones de gestión específicas encaminadas a supervisar los acuerdos con proveedores terceros de servicios de TIC o a abordar la gestión de crisis, para organizar su gestión de riesgos relacionados con las TIC con arreglo al modelo de tres líneas de defensa o para establecer un modelo interno de control y gestión de riesgos, y para someter a auditorías internas su marco de gestión de riesgos relacionados con las TIC.

(39) Algunas entidades financieras se benefician de exenciones o están sujetas a un marco regulador poco estricto con arreglo al Derecho sectorial pertinente de la Unión. Entre esas entidades financieras se encuentran los gestores de fondos de inversión alternativos a que se refiere el artículo 3, apartado 2, de la Directiva 2011/61/UE del Parlamento Europeo y del Consejo ([16]), las empresas de seguros y reaseguros a que se refiere el artículo 4 de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo ([17]), y los fondos de pensiones de empleo que

([14]) Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, p. 7).

([15]) Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

([16]) Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) n.º 1060/2009 y (UE) n.º 1095/2010 (DO L 174 de 1.7.2011, p. 1).

([17]) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1).

gestionen planes de pensiones que, en conjunto, no tengan más de quince partícipes en total. A la luz de esas exenciones, sería desproporcionado incluir a dichas entidades financieras en el ámbito de aplicación del presente Reglamento. Además, el presente Reglamento reconoce las especificidades de la estructura del mercado de la intermediación de seguros, con la consecuencia de que los intermediarios de seguros, los intermediarios de reaseguros y los intermediarios de seguros complementarios considerados microempresas o pequeñas o medianas empresas no deben estar sujetos al presente Reglamento.

(40) Dado que las entidades a que se refiere el artículo 2, apartado 5, puntos 4 a 23, de la Directiva 2013/36/UE están excluidas del ámbito de aplicación de dicha Directiva, los Estados miembros deben poder optar por eximir de la aplicación del presente Reglamento a dichas entidades situadas en sus respectivos territorios.

(41) Del mismo modo, a fin de adaptar el presente Reglamento al ámbito de aplicación de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo ([18]), también conviene excluir del ámbito de aplicación del presente Reglamento a las personas físicas y jurídicas a que se refieren los artículos 2 y 3 de dicha Directiva que estén autorizadas a prestar servicios de inversión sin tener que obtener una autorización con arreglo a la Directiva 2014/65/UE. No obstante, el artículo 2 de la Directiva 2014/65/UE también excluye del ámbito de aplicación de dicha Directiva a las entidades que puedan considerarse entidades financieras a efectos del presente Reglamento, como los depositarios centrales de valores, las instituciones de inversión colectiva o las empresas de seguros y de reaseguros. La exclusión del ámbito de aplicación del presente Reglamento de las personas y entidades a que se refieren los artículos 2 y 3 de dicha Directiva no debe abarcar a esos depositarios centrales de valores, instituciones de inversión colectiva o empresas de seguros y de reaseguros.

(42) Con arreglo al Derecho sectorial de la Unión, algunas entidades financieras están sujetas a requisitos o exenciones menos estrictos por motivos relacionados con su tamaño o con los servicios que prestan. Entre esta categoría de entidades financieras se encuentran las empresas de servicios de inversión pequeñas y no interconectadas, los fondos de pensiones de empleo pequeños que pueden quedar excluidos con arreglo a la Directiva (UE) 2016/2341 en las condiciones establecidas en el artículo 5 de dicha Directiva por el Estado miembro de que se trate y que gestionan planes de pensiones que, en conjunto, no tengan más de cien partícipes, así como las entidades exentas en virtud de la Directiva 2013/36/UE. Por consiguiente, de conformidad con el principio de proporcionalidad y con el fin de preservar el espíritu del Derecho sectorial de la Unión, también conviene someter a dichas entidades financieras a un marco simplificado de gestión del riesgo relacionado con las TIC con arreglo al presente Reglamento. El carácter proporcionado del marco de gestión del riesgo relacionado con las TIC que abarca a esas entidades financieras no debe verse alterado por las normas técnicas de regulación que deben desarrollar las Autoridades Europeas de Supervisión. Además, de conformidad con el principio de proporcionalidad, conviene someter también a las entidades de pago a que se refiere el artículo 32, apartado 1, de la Directiva (UE) 2015/2366 y a las entidades de dinero electrónico a que se refiere el artículo 9 de la Directiva 2009/110/CE, exentas de conformidad con el Derecho nacional por el que se transpongan estos actos jurídicos de la Unión a un marco simplificado de gestión del riesgo relacionado con las TIC con arreglo al presente Reglamento, mientras que las entidades de pago y las entidades de dinero electrónico que no hayan sido eximidas de conformidad con su respectivo Derecho nacional por el que se transponga el Derecho sectorial de la Unión deben cumplir el marco general establecido en el presente Reglamento.

(43) De modo similar, las entidades financieras que se consideran microempresas o que están sujetas al marco simplificado de gestión del riesgo relacionado con las TIC con arreglo al presente Reglamento no deben estar obligadas a crear un cargo para el seguimiento de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC; a designar a un miembro de la alta dirección para que sea responsable de supervisar la exposición al riesgo correspondiente y la documentación pertinente; a asignar la responsabilidad de la gestión y supervisión del riesgo relacionado con las TIC a una función de control y garantizar un nivel adecuado de independencia de dicha función de control para evitar conflictos de intereses; a documentar y revisar al menos una vez al año el marco de gestión del riesgo relacionado con las TIC; a someter a auditoría interna periódicamente el marco de gestión del riesgo relacionado con las TIC; a llevar a cabo evaluaciones exhaustivas tras cambios importantes en los procesos y las infraestructuras de su red y sistemas de información; a realizar periódicamente análisis de riesgos sobre los sistemas de TIC heredados; a someter a auditorías internas independientes la ejecución de los planes de respuesta y recuperación en materia de TIC; a disponer de una función de gestión de crisis; a ampliar las pruebas sobre los planes de continuidad de la actividad y de respuesta y recuperación para reflejar los escenarios de conmutación entre la infraestructura primaria de TIC y las instalaciones redundantes; a comunicar a

([18]) 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).

las autoridades competentes que lo soliciten una estimación de los costes y pérdidas anuales agregados provocados por incidentes graves relacionados con las TIC, a mantener capacidades de TIC redundantes; a comunicar a las autoridades nacionales competentes los cambios ejecutados a raíz de revisiones realizadas tras incidentes relacionados con las TIC; a hacer un seguimiento continuo de los avances tecnológicos pertinentes; a establecer un programa completo de pruebas de resiliencia operativa digital como parte integrante del marco de gestión del riesgo relacionado con las TIC establecido en el presente Reglamento, o a adoptar y revisar periódicamente una estrategia relativa al riesgo relacionado con las TIC derivado de terceros. Además, se debe obligar a las microempresas a que evalúen la necesidad de mantener estas capacidades de TIC redundantes únicamente sobre la base de su perfil de riesgo. Las microempresas deben beneficiarse de un régimen más flexible en lo que respecta a los programas de pruebas de resiliencia operativa digital. A la hora de considerar el tipo y la frecuencia de las pruebas que han de realizarse, deben buscar un equilibrio adecuado entre el objetivo de mantener una elevada resiliencia operativa digital, los recursos disponibles y su perfil de riesgo general. Las microempresas y las entidades financieras sujetas al marco simplificado de gestión del riesgo relacionado con las TIC con arreglo al presente Reglamento deben quedar exentas del requisito de realizar pruebas avanzadas de herramientas, sistemas y procesos de TIC sobre la base de pruebas de penetración basadas en amenazas, ya que solo las entidades financieras que cumplen los criterios establecidos en el presente Reglamento deben estar obligadas a llevar a cabo dichas pruebas. Habida cuenta de sus limitadas capacidades, las microempresas deben poder acordar con el proveedor tercero de servicios de TIC la delegación de los derechos de acceso, inspección y auditoría de la entidad financiera en un tercero independiente, que nombrará el proveedor tercero de servicios de TIC, siempre que la entidad financiera pueda solicitar, en cualquier momento, toda la información y garantías pertinentes sobre el rendimiento del proveedor tercero de servicios de TIC al tercero independiente respectivo.

(44) Dado que solo las entidades financieras identificadas a efectos de las pruebas avanzadas de resiliencia digital deben estar obligadas a llevar a cabo pruebas de penetración basadas en amenazas, los procesos administrativos y los costes financieros derivados de la realización de dichas pruebas deben recaer en un pequeño porcentaje de entidades financieras.

(45) Para garantizar la plena armonización y la coherencia general entre las estrategias empresariales de las entidades financieras, por una parte, y la gestión del riesgo relacionado con las TIC, por otra, debe exigirse a los órganos de dirección de las entidades financieras que desempeñen un papel central y activo en la dirección y adaptación del marco de gestión del riesgo relacionado con las TIC y de la estrategia de resiliencia digital general. El enfoque que adopten los órganos de dirección no solo debe centrarse en los medios para garantizar la resiliencia de los sistemas de TIC, sino que también debe abarcar a las personas y los procesos a través de un conjunto de políticas que promuevan, en cada nivel corporativo y para todo el personal, una fuerte concienciación sobre los riesgos de ciberseguridad y el compromiso de respetar una estricta ciberhigiene a todos los niveles. La responsabilidad última del órgano de dirección en la gestión del riesgo relacionado con las TIC de una entidad financiera debe ser un principio fundamental de ese enfoque global, que se traducirá además en la implicación continua del órgano de dirección en el control del seguimiento de la gestión del riesgo relacionado con las TIC.

(46) Además, el principio de la responsabilidad plena y última del órgano de dirección sobre la gestión del riesgo relacionado con las TIC de la entidad financiera va acompañado de la necesidad de garantizar un nivel de inversiones relacionadas con las TIC y un presupuesto global para la entidad financiera que permita que esta alcance un elevado nivel de resiliencia operativa digital.

(47) Inspirándose en las pertinentes buenas prácticas, directrices, recomendaciones y enfoques internacionales, nacionales y sectoriales en relación con la gestión del riesgo cibernético, el presente Reglamento promueve una serie de principios que facilitan la estructura general de la gestión del riesgo relacionado con las TIC. Por consiguiente, mientras las principales capacidades que las entidades financieras ponen en práctica aborden las distintas funciones de la gestión del riesgo relacionado con las TIC (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución y comunicación) establecidas en el presente Reglamento, las entidades financieras deben seguir teniendo libertad para utilizar modelos de gestión del riesgo relacionado con las TIC que se enmarquen o categoricen de manera diferente.

(48) Para seguir el ritmo de la evolución del panorama de las ciberamenazas, las entidades financieras deben mantener sistemas de TIC actualizados que sean fiables y capaces, no solo de garantizar el tratamiento de datos necesario para sus servicios, sino también de asegurar una resiliencia tecnológica suficiente que les permita ocuparse adecuadamente de las necesidades de tratamiento adicionales debidas al tensionamiento del mercado o a otras situaciones adversas.

(49) Son necesarios planes eficientes de continuidad de la actividad y de recuperación para que las entidades financieras puedan resolver pronta y rápidamente los incidentes relacionados con las TIC, en particular los ciberataques, limitando los daños y dando prioridad a la reanudación de las actividades y a las acciones de recuperación de conformidad con sus políticas de respaldo. No obstante, dicha reanudación no debe en modo alguno poner en peligro la integridad y la seguridad de las redes y los sistemas de información ni la disponibilidad, autenticidad, integridad o confidencialidad de los datos.

(50) Si bien el presente Reglamento permite a las entidades financieras determinar de manera flexible sus objetivos de tiempo de recuperación y punto de recuperación y, por tanto, fijar tales objetivos teniendo plenamente en cuenta la naturaleza y el carácter esencial de las funciones pertinentes y cualesquiera necesidades empresariales específicas, al determinar dichos objetivos les debe exigir, no obstante, la realización de una evaluación del posible impacto global en la eficiencia del mercado.

(51) Los propagadores de ciberataques tienden a perseguir la obtención de beneficios financieros directamente en la fuente, exponiendo así a las entidades financieras a consecuencias importantes. Para impedir que los sistemas de TIC pierdan integridad o dejen de estar disponibles y evitar así que se vulneren datos y que sufran daños las infraestructuras físicas de TIC, debe mejorarse y racionalizarse significativamente la notificación de incidentes graves relacionados con las TIC por parte de las entidades financieras. La notificación de incidentes relacionados con las TIC debe armonizarse mediante la introducción del requisito de que todas las entidades financieras informen directamente a sus autoridades competentes pertinentes. Cuando una entidad financiera esté sujeta a la supervisión de más de una autoridad nacional competente, los Estados miembros deben designar a una única autoridad competente como destinataria de dicha información. Las entidades de crédito clasificadas como significativas de conformidad con el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013 del Consejo ([19]) deben presentar dicha información a las autoridades nacionales competentes, que deben transmitir posteriormente el informe al Banco Central Europeo (BCE).

(52) La notificación directa debe posibilitar que los supervisores financieros tengan acceso inmediato a información sobre incidentes graves relacionados con las TIC. Los supervisores financieros deben a su vez transmitir los detalles de incidentes graves relacionados con las TIC a las autoridades no financieras públicas (como las autoridades competentes y los puntos de contacto únicos con arreglo a la Directiva (UE) 2022/2555, las autoridades nacionales de protección de datos y las autoridades policiales en caso de incidentes graves relacionados con las TIC que tengan carácter delictivo) a fin de mejorar el conocimiento que dichas autoridades tienen de tales incidentes y, en el caso de los equipos de respuesta a incidentes de seguridad informática, facilitar la asistencia rápida que pueda prestarse a las entidades financieras, según proceda. Además, los Estados miembros deben poder determinar que las propias entidades financieras faciliten dicha información a las autoridades públicas fuera del ámbito de los servicios financieros. Dichos flujos de información deben permitir a las entidades financieras beneficiarse rápidamente de cualquier aportación técnica pertinente, asesoramiento sobre medidas correctoras y seguimiento posterior por parte de dichas autoridades. La información sobre incidentes graves relacionados con las TIC debe comunicarse recíprocamente: los supervisores financieros deben proporcionar a la entidad financiera todas las observaciones u orientaciones necesarias, mientras que las Autoridades Europeas de Supervisión deben compartir datos anonimizados sobre ciberamenazas y vulnerabilidades relacionadas con un determinado incidente, con el fin de contribuir a una defensa colectiva más amplia.

(53) Aunque debe exigirse a todas las entidades financieras que notifiquen los incidentes, no se espera que todas ellas se vean afectadas de la misma manera por este requisito. En efecto, los umbrales de importancia relativa, así como los plazos de notificación, deben ajustarse debidamente en el contexto de los actos delegados basados en las normas técnicas de regulación que deben desarrollar las Autoridades Europeas de Supervisión, con el fin de cubrir únicamente los incidentes graves relacionados con las TIC. Además, deben tenerse en cuenta las particularidades de las entidades financieras a la hora de establecer plazos para las obligaciones de notificación.

(54) El presente Reglamento debe exigir a las entidades de crédito, a las entidades de pago, a los proveedores de servicios de información sobre cuentas y a las entidades de dinero electrónico que notifiquen todos los incidentes operativos o de seguridad relacionados con los pagos —previamente notificados con arreglo a la Directiva (UE) 2015/2366— con independencia de si la naturaleza del incidente está relacionada con las TIC.

([19]) Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito (DO L 287 de 29.10.2013, p. 63).

(55) Debe encargarse a las Autoridades Europeas de Supervisión que evalúen la viabilidad y las condiciones para una posible centralización de los informes de incidentes relacionados con las TIC a escala de la Unión. Dicha centralización puede consistir en un centro único de la UE para la notificación de incidentes graves relacionados con las TIC que reciba directamente los informes pertinentes y los notifique automáticamente a las autoridades nacionales competentes, o que simplemente centralice los informes pertinentes transmitidos por las autoridades nacionales competentes y desempeñe de este modo una función de coordinación. Debe encargarse a las Autoridades Europeas de Supervisión que elaboren, en consulta con el BCE y la ENISA, un informe conjunto en el que se estudie la viabilidad de crear un centro único de la UE.

(56) Con el fin de lograr un nivel elevado de resiliencia operativa digital, y en consonancia tanto con las normas internacionales pertinentes (por ejemplo, los Elementos Fundamentales del G7 para las pruebas de penetración basadas en amenazas) como con los marcos aplicados en la Unión, como el TIBER-EU, las entidades financieras deben someter a pruebas periódicas a sus sistemas de TIC y a su personal con responsabilidades relacionadas con las TIC en lo que respecta a la efectividad de sus capacidades de prevención, detección, respuesta y recuperación, a fin de descubrir y abordar posibles vulnerabilidades de las TIC. Para reflejar las diferencias que existen entre los distintos subsectores financieros y dentro de ellos en relación con el nivel de preparación de las entidades financieras en materia de ciberseguridad, las pruebas deben incluir una amplia variedad de herramientas y acciones, que van desde la evaluación de los requisitos básicos (por ejemplo, evaluaciones y exploraciones de vulnerabilidad, análisis del código abierto, evaluaciones de la seguridad de la red, análisis de carencias, revisiones de seguridad física, cuestionarios y soluciones de *software* de exploración, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento o pruebas de extremo a extremo) hasta pruebas más avanzadas a través de pruebas de penetración basadas en amenazas. Estas pruebas avanzadas solo deben exigirse a las entidades financieras que sean suficientemente maduras desde la perspectiva de las TIC para llevarlas a cabo razonablemente. Las pruebas de resiliencia operativa digital exigidas por el presente Reglamento deben, por tanto, ser más exigentes para las entidades financieras significativas (como grandes entidades de crédito, bolsas de valores, depositarios centrales de valores, entidades de contrapartida central, etc.) que para otras entidades financieras. Al mismo tiempo, las pruebas de resiliencia operativa digital por medio de pruebas de penetración basadas en amenazas deben ser más pertinentes para las entidades financieras que operen en subsectores esenciales de los servicios financieros y que desempeñen un papel sistémico (por ejemplo, pagos, banca, compensación y liquidación) y menos pertinentes para otros subsectores (por ejemplo, gestores de activos, agencias de calificación crediticia, etc.).

(57) Las entidades financieras que participen en actividades transfronterizas y que ejerzan la libertad de establecimiento o prestación de servicios en la Unión deben cumplir un único conjunto de requisitos de pruebas avanzadas (por ejemplo, pruebas de penetración basadas en amenazas) en su Estado miembro de origen, el cual debe incluir las infraestructuras de TIC en todos los países o territorios en los que el grupo financiero transfronterizo opere dentro de la Unión, permitiendo así que los grupos financieros transfronterizos solo soporten los costes de las pruebas relacionadas con las TIC en un país o territorio.

(58) A fin de aprovechar los conocimientos especializados ya adquiridos por determinadas autoridades competentes, en particular en lo que se refiere a la aplicación del marco TIBER-EU, el presente Reglamento debe permitir que los Estados miembros designen a una única autoridad pública como responsable en el sector financiero, a escala nacional, para todas las cuestiones relacionadas con las pruebas de penetración basadas en amenazas, o que las autoridades competentes deleguen, a falta de dicha designación, el ejercicio de las tareas relacionadas con las pruebas de penetración basadas en amenazas en otra autoridad financiera nacional competente.

(59) Dado que el presente Reglamento no exige que las entidades financieras abarquen todas las funciones esenciales o importantes en una única prueba de penetración basada en amenazas, las entidades financieras deben tener libertad para determinar las funciones esenciales o importantes que deben incluirse en el ámbito de aplicación de tal prueba y cuántas de dichas funciones.

(60) Se autorizan las pruebas conjuntas en el sentido del presente Reglamento —en las que varias entidades financieras participan en una prueba de penetración basada en amenazas y para las cuales un proveedor tercero de servicios de TIC puede celebrar directamente acuerdos contractuales con un probador externo— solo en aquellos casos en los que cabe esperar razonablemente que se vean afectadas negativamente la calidad o la seguridad de los servicios prestados por el proveedor tercero de servicios de TIC a clientes que son entidades excluidas del ámbito de aplicación del presente Reglamento, o la confidencialidad de los datos relacionados con tales servicios. Las pruebas conjuntas también deben estar sujetas a salvaguardias (dirección a cargo de una entidad financiera designada, determinación del número de entidades financieras participantes) a fin de garantizar el rigor de la prueba para que las entidades financieras implicadas cumplan los objetivos de la prueba de penetración basada en amenazas en virtud del presente Reglamento.

(61) Con el fin de aprovechar los recursos internos disponibles a escala corporativa, el presente Reglamento debe permitir el recurso a probadores internos para llevar a cabo pruebas de penetración basadas en amenazas, siempre que se cuente con la aprobación de las autoridades de control, no existan conflictos de interés y se alterne periódicamente el recurso a probadores internos y externos (cada tres pruebas), al tiempo que se exige que el proveedor de inteligencia sobre amenazas en dichas pruebas de penetración sea siempre externo a la entidad financiera. La responsabilidad de llevar a cabo las pruebas de penetración basadas en amenazas debe seguir recayendo plenamente en la entidad financiera. Las validaciones proporcionadas por las autoridades deben tener como única finalidad el reconocimiento mutuo y no deben impedir ninguna acción de seguimiento necesaria para abordar el riesgo en materia de TIC al que esté expuesta la entidad financiera, ni deben considerarse como una confirmación por parte de las autoridades de control de las capacidades de gestión y mitigación del riesgo de TIC de una entidad financiera.

(62) Para garantizar un seguimiento sólido del riesgo relacionado con las TIC derivado de terceros en el sector financiero, es necesario establecer un conjunto de normas basadas en principios para orientar a las entidades financieras a la hora de hacer un seguimiento de los riesgos que surgen en el contexto de las funciones externalizadas a proveedores terceros de servicios de TIC, en particular para servicios de TIC que den apoyo a funciones esenciales o importantes, así como, de manera más general, en el contexto de todas las dependencias de terceros relacionadas con las TIC.

(63) Para abordar la complejidad de las diversas fuentes de riesgo relacionado con las TIC, teniendo en cuenta al mismo tiempo la multitud y diversidad de proveedores de soluciones tecnológicas que hacen posible una prestación fluida de los servicios financieros, el presente Reglamento debe abarcar una amplia variedad de proveedores terceros de servicios de TIC, incluidos los proveedores de servicios de computación en nube, *software*, servicios de análisis de datos y los proveedores de servicios de centros de datos. Del mismo modo, dado que las entidades financieras deben determinar y gestionar de manera efectiva y coherente todos los tipos de riesgo, también en el contexto de los servicios de TIC adquiridos dentro de un grupo financiero, debe aclararse que las empresas que forman parte de un grupo financiero y prestan servicios de TIC principalmente a su sociedad matriz, o a filiales o sucursales de su empresa matriz, así como las entidades financieras que prestan servicios de TIC a otras entidades financieras, también deben considerarse proveedores terceros de servicios de TIC de conformidad con el presente Reglamento. Por último, a la luz de la evolución del mercado de servicios de pago, cada vez más dependiente de soluciones técnicas complejas, y en vista de los nuevos tipos de servicios de pago y soluciones relacionadas con los pagos, los participantes en el ecosistema de servicios de pago que presten actividades de procesamiento de pagos o gestionen infraestructuras también deben considerarse proveedores terceros de servicios de TIC con arreglo al presente Reglamento, a excepción de los bancos centrales cuando gestionen sistemas de pago o de liquidación de valores y las autoridades públicas cuando presten servicios relacionados con las TIC en el contexto del desempeño de funciones estatales.

(64) Una entidad financiera debe seguir siendo en todo momento plenamente responsable del cumplimiento de las obligaciones que respecto de ella se establecen en el presente Reglamento. Las entidades financieras deben aplicar un enfoque proporcionado al seguimiento de los riesgos que surjan a nivel de los proveedores terceros de servicios de TIC teniendo debidamente en cuenta la naturaleza, la escala, la complejidad y la importancia de sus dependencias relacionadas con las TIC, el carácter esencial o la importancia de los servicios, procesos o funciones sujetos a los acuerdos contractuales y, en última instancia, sobre la base de una evaluación cuidadosa de cualquier posible consecuencia para la continuidad y calidad de los servicios financieros a escala particular y de grupo, según proceda.

(65) La realización de dicho seguimiento debe seguir un enfoque estratégico para el riesgo relacionado con las TIC derivado de terceros formalizado mediante la adopción por parte del órgano de dirección de la entidad financiera de una estrategia de riesgos relacionados con las TIC derivados de terceros específica, basada en un examen continuo de todas las dependencias de terceros relacionadas con las TIC. Para aumentar la sensibilización entre las autoridades de control sobre las dependencias de terceros en el sector de las TIC, y con vistas a apoyar en mayor medida el trabajo desarrollado en el contexto del marco de supervisión establecido por el presente Reglamento, debe exigirse a todas las entidades financieras que mantengan un registro de información con todos los acuerdos contractuales relativos al uso de servicios de TIC prestados por proveedores terceros de servicios de TIC. Los supervisores financieros deben poder solicitar el registro completo o solicitar secciones específicas de este, y así obtener información esencial para adquirir una mayor comprensión de las dependencias relacionadas con las TIC de las entidades financieras.

(66) La celebración formal de acuerdos contractuales debe fundarse e ir precedida de un análisis exhaustivo previo a la contratación, centrado en particular en elementos como el carácter esencial o la importancia de los servicios cubiertos por el contrato de TIC previsto, las aprobaciones de las autoridades de control necesarias u otras condiciones, el posible riesgo de concentración que conlleva, aplicando asimismo la diligencia debida en el proceso de selección y evaluación de los proveedores terceros de servicios de TIC y evaluando los posibles conflictos de intereses. En lo que respecta a los acuerdos contractuales relativos a funciones esenciales o importantes, las entidades financieras deben tener en cuenta el uso por parte de los proveedores terceros de servicios de TIC de los estándares más actualizados y más estrictos en materia de seguridad de la información. La terminación de los

contratos puede estar motivada como mínimo, por una serie de circunstancias que pongan de manifiesto deficiencias a nivel del proveedor tercero de servicios de TIC, en particular incumplimientos importantes de leyes o de cláusulas contractuales, circunstancias que revelen una posible alteración en el desempeño de las funciones contempladas en el contrato, pruebas de deficiencias del proveedor tercero de servicios de TIC en su gestión global de riesgos de TIC, o circunstancias que indiquen la incapacidad de la autoridad competente pertinente para supervisar eficazmente la entidad financiera.

(67) Para abordar las repercusiones sistémicas del riesgo de concentración de terceros en el ámbito de las TIC, el presente Reglamento promueve una solución equilibrada mediante la adopción de un enfoque flexible y gradual en lo que respecta a dicho riesgo de concentración, ya que la imposición de unos techos rígidos o unas limitaciones estrictas podría obstaculizar la actividad empresarial y restringir la libertad contractual. Las entidades financieras deben evaluar exhaustivamente los acuerdos contractuales que tienen previstos para determinar la probabilidad de que aparezca dicho riesgo, también mediante análisis en profundidad de los acuerdos de subcontratación, en particular cuando se celebren con proveedores terceros de servicios de TIC establecidos en un tercer país. En esta fase, y con el fin de lograr un equilibrio justo entre el imperativo de preservar la libertad contractual y el de garantizar la estabilidad financiera, no se considera apropiado establecer normas sobre techos y límites estrictos a las exposiciones frente a terceros en el ámbito de las TIC. En el contexto del marco de supervisión, un supervisor principal nombrado en virtud del presente Reglamento debe, en relación con los proveedores terceros esenciales de servicios de TIC, prestar especial atención a comprender plenamente la magnitud de las interdependencias, descubrir los casos específicos en los que un alto grado de concentración de proveedores terceros esenciales de servicios de TIC en la Unión pueda poner bajo presión la estabilidad e integridad del sistema financiero de la Unión y mantener un diálogo con los proveedores terceros esenciales de servicios de TIC cuando se detecte ese riesgo específico.

(68) Para evaluar y controlar periódicamente la capacidad del proveedor tercero de servicios de TIC para prestar servicios de forma segura a la entidad financiera sin que ello produzca efectos adversos para la capacidad de resiliencia operativa digital de esta, deben armonizarse varios elementos contractuales fundamentales con los proveedores terceros de servicios de TIC. Dicha armonización debe cubrir ámbitos mínimos que son cruciales para que la entidad financiera pueda hacer un seguimiento completo de los riesgos que podrían derivarse del proveedor tercero de servicios de TIC desde la perspectiva de la necesidad de una entidad financiera de garantizar su resiliencia digital por depender en gran medida de la estabilidad, la funcionalidad, la disponibilidad y la seguridad de los servicios de TIC recibidos.

(69) Al renegociar los acuerdos contractuales para conformarlos con los requisitos establecidos en el presente Reglamento, las entidades financieras y los proveedores terceros de servicios de TIC deben garantizar que quedan cubiertas las cláusulas contractuales fundamentales contempladas en el presente Reglamento.

(70) La definición de «función esencial o importante» establecida en el presente Reglamento engloba la definición de «funciones esenciales» del artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE del Parlamento Europeo y del Consejo ([20]). De este modo, las funciones que se consideran esenciales en virtud de la citada Directiva se incluyen en la definición de funciones esenciales o importantes en el sentido del presente Reglamento.

(71) Independientemente del carácter esencial o de la importancia de la función sustentada por los servicios de TIC, los acuerdos contractuales deben especificar, en particular, las descripciones completas de las funciones y servicios, de los lugares en los que se presten tales funciones y en los que se procesarán los datos, así como una indicación de las descripciones de los niveles de servicio. Otros elementos esenciales para permitir el seguimiento por parte de la entidad financiera del riesgo relacionado con las TIC derivado de terceros son las disposiciones contractuales que especifiquen el modo en que el proveedor tercero de servicios de TIC garantiza la accesibilidad, la disponibilidad, la integridad, la seguridad y la protección de los datos personales; las disposiciones que establecen las garantías pertinentes para permitir el acceso, la recuperación y la restitución de los datos en caso de insolvencia, resolución o interrupción de las operaciones comerciales del proveedor tercero de servicios de TIC, así como las disposiciones que obligan al proveedor tercero de servicios de TIC a prestar asistencia en caso de incidentes relacionados con las TIC

([20]) Directiva 2014/59/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, por la que se establece un marco para la recuperación y la resolución de entidades de crédito y empresas de servicios de inversión, y por la que se modifican la Directiva 82/891/CEE del Consejo, y las Directivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE y 2013/36/UE, y los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 648/2012 del Parlamento Europeo y del Consejo (DO L 173 de 12.6.2014, p. 190).

vinculados a los servicios prestados, sin coste adicional o con un coste determinado con anterioridad; las disposiciones relativas a la obligación del proveedor tercero de servicios de TIC de cooperar plenamente con las autoridades competentes y las autoridades de resolución de la entidad financiera; y las disposiciones relativas a los derechos de terminación y los correspondientes plazos mínimos de notificación para la terminación de los acuerdos contractuales, con arreglo a las expectativas de las autoridades competentes y de las autoridades de resolución.

(72) Además de estas disposiciones contractuales, y con vistas a garantizar que las entidades financieras mantengan el pleno control de todos los acontecimientos que se produzcan a nivel de terceros que puedan perjudicar su seguridad en materia de TIC, los contratos para la prestación de servicios de TIC que sustenten funciones esenciales o importantes también deben establecer lo siguiente: la especificación de las descripciones completas del nivel de servicio, con objetivos de rendimiento cuantitativos y cualitativos precisos, para permitir, sin demora indebida, la adopción de medidas correctoras adecuadas cuando no se alcancen los niveles de servicio acordados; los plazos de notificación y las obligaciones de información pertinentes de los proveedores terceros de servicios de TIC en caso de cambios que puedan tener consecuencias importantes para la capacidad del proveedor tercero de servicios de TIC de prestar efectivamente sus servicios de TIC respectivos; la obligación para el proveedor tercero de servicios de TIC de aplicar y someter a prueba los planes de contingencia empresariales y disponer de medidas, herramientas y políticas de seguridad de las TIC que permitan la prestación segura de servicios, y de participar y cooperar plenamente en la prueba de penetración basada en amenazas llevada a cabo por la entidad financiera.

(73) Los contratos para la prestación de servicios de TIC que sustenten funciones esenciales o importantes deben contener también disposiciones que estipulen derechos de acceso, inspección y auditoría por parte de la entidad financiera o de un tercero designado, y el derecho de hacer copias, como instrumentos cruciales para las entidades financieras a la hora de hacer un seguimiento permanente del rendimiento del proveedor tercero de servicios de TIC, junto con la plena cooperación de este último durante las inspecciones. Del mismo modo, la autoridad competente de la entidad financiera debe tener el derecho de inspeccionar y auditar, previa notificación, al proveedor tercero de servicios de TIC, a reserva de la protección de la información confidencial.

(74) Dichos acuerdos contractuales deben estipular también estrategias específicas de salida que permitan establecer, en particular períodos transitorios obligatorios durante los cuales los proveedores terceros de servicios de TIC deben seguir proporcionando los servicios pertinentes con vistas a reducir el riesgo de perturbaciones a nivel de la entidad financiera, o para permitir que esta última cambie de modo efectivo de proveedores terceros de servicios de TIC o, alternativamente, opte por soluciones internas, en consonancia con la complejidad del servicio de TIC prestado. Además, las entidades financieras incluidas en el ámbito de aplicación de la Directiva 2014/59/UE deben garantizar que los contratos de servicios de TIC pertinentes sean sólidos y plenamente aplicables en caso de resolución de dichas entidades financieras. Por consiguiente, en consonancia con las expectativas de las autoridades de resolución, estas entidades financieras deben garantizar que los contratos de servicios de TIC correspondientes sean resilientes a las resoluciones. Mientras sigan cumpliendo sus obligaciones de pago, estas entidades financieras deben garantizar, entre otros requisitos, que los contratos pertinentes de servicios de TIC contengan cláusulas de no terminación, no suspensión y no modificación por motivos de reestructuración o resolución.

(75) Además, la inclusión voluntaria de cláusulas contractuales tipo desarrolladas por autoridades públicas o instituciones de la Unión, en particular la inclusión de cláusulas contractuales desarrolladas por la Comisión para los servicios de computación en nube, puede ofrecer mayor confianza a las entidades financieras y a los proveedores terceros de servicios de TIC al aumentar su nivel de seguridad jurídica en lo concerniente al uso de servicios de computación en nube en el sector financiero, respetando plenamente los requisitos y expectativas establecidos en el Derecho de la Unión en materia de servicios financieros. El desarrollo de cláusulas contractuales tipo se basa en las medidas ya previstas en el Plan de Acción en materia de Tecnología Financiera de 2018, que anunciaba la intención de la Comisión de fomentar y facilitar el desarrollo de cláusulas contractuales tipo para la externalización de servicios de computación en nube por parte de las entidades financieras, basándose en los esfuerzos intersectoriales de las partes interesadas del ámbito de los servicios de computación en nube, que la Comisión ha facilitado con la ayuda de la participación del sector financiero.

(76) Los proveedores terceros esenciales de servicios de TIC deben estar sujetos a un marco de supervisión con vistas a promover la convergencia y la eficiencia en relación con los enfoques de supervisión a la hora de afrontar el riesgo relacionado con las TIC derivado de terceros en el sector financiero, así como para reforzar la resiliencia operativa digital de las entidades financieras que dependen de proveedores terceros esenciales de servicios de TIC para la prestación de servicios de TIC que sustentan la prestación de servicios financieros, y contribuir así a preservar la estabilidad del sistema financiero de la Unión y la integridad del mercado único de servicios financieros. Si bien el establecimiento del marco de supervisión se justifica por el valor añadido de la adopción de medidas a escala de la

Unión y por el papel inherente y las especificidades del uso de los servicios de TIC en la prestación de servicios financieros, debe recordarse, al mismo tiempo, que esta solución parece adecuada únicamente en el contexto del presente Reglamento, que aborda específicamente la resiliencia operativa digital en el sector financiero. No obstante, este marco de supervisión no debe considerarse como un nuevo modelo para la supervisión por la Unión en otros ámbitos de los servicios y actividades financieros.

(77) El marco de supervisión debe aplicarse únicamente a los proveedores terceros esenciales de servicios de TIC. Por consiguiente, debe existir un mecanismo de designación que tenga en cuenta la dimensión y la naturaleza de la dependencia del sector financiero de dichos proveedores terceros de servicios de TIC. Dicho mecanismo debe comportar un conjunto de criterios cuantitativos y cualitativos para establecer los parámetros para determinar el carácter esencial como base para la inclusión en el marco de supervisión. A fin de garantizar la exactitud de dicha evaluación, y con independencia de la estructura corporativa del proveedor tercero de servicios de TIC, tales criterios, en el caso de un proveedor tercero de servicios de TIC que forme parte de un grupo más amplio, deben tener en cuenta toda la estructura del grupo del proveedor tercero de servicios de TIC. Por una parte, los proveedores terceros esenciales de servicios de TIC que no sean designados automáticamente en virtud de la aplicación de estos criterios deben tener la posibilidad de participar voluntariamente en el marco de supervisión, mientras que, por otra parte, los proveedores terceros de servicios de TIC que ya estén sujetos a marcos del mecanismo de supervisión que apoyan el desempeño de las tareas del Sistema Europeo de Bancos Centrales a que se refiere el artículo 127, apartado 2, del TFUE, deben quedar exentos.

(78) Del mismo modo, las entidades financieras que prestan servicios de TIC a otras entidades financieras, aunque pertenezcan a la categoría de proveedores terceros de servicios de TIC con arreglo al presente Reglamento, también deben quedar exentas del marco de supervisión, puesto que ya están sujetas a mecanismos de control establecidos por el Derecho de la Unión aplicable en materia de servicios financieros. Cuando proceda, las autoridades competentes deben tener en cuenta, en el contexto de sus actividades de control, el riesgo relacionado con las TIC que plantean para las entidades financieras las entidades financieras que prestan servicios de TIC. Del mismo modo, debido a los mecanismos de seguimiento de riesgos existentes a escala de grupo, debe introducirse la misma exención para los proveedores terceros de servicios de TIC que presten servicios predominantemente a las entidades de su propio grupo. Los proveedores terceros de servicios de TIC que presten servicios de TIC únicamente en un Estado miembro a entidades financieras que solo operen en ese Estado también deben quedar exentos del mecanismo de designación debido al carácter limitado de sus actividades y a la ausencia de consecuencias transfronterizas.

(79) La transformación digital experimentada en los servicios financieros ha dado lugar a un nivel de uso y dependencia de los servicios de TIC que no tiene precedentes. Dado que hoy en día resulta inconcebible prestar servicios financieros sin el uso de servicios de computación en nube, soluciones de *software* y servicios relacionados con datos, el ecosistema financiero de la Unión ha pasado a ser intrínsecamente codependiente de determinados servicios de TIC prestados por proveedores de servicios de TIC. Algunos de estos proveedores, innovadores en el desarrollo y la aplicación de tecnologías basadas en las TIC, desempeñan un papel importante en la prestación de servicios financieros o se han integrado en la cadena de valor de los servicios financieros. Por lo tanto, se han convertido en fundamentales para la estabilidad y la integridad del sistema financiero de la Unión. Esta dependencia generalizada de los servicios prestados por proveedores terceros esenciales de servicios de TIC, combinada con la interdependencia de los sistemas de información de diversos operadores del mercado, crea un riesgo directo y potencialmente grave para el sistema de servicios financieros de la Unión y para la continuidad de la prestación de servicios financieros en caso de que los proveedores terceros esenciales de servicios de TIC se vean afectados por perturbaciones operativas o por ciberincidentes graves. Los ciberincidentes tienen una capacidad particular para multiplicarse y propagarse por todo el sistema financiero a un ritmo considerablemente más rápido que otros tipos de riesgos sujetos a seguimiento en el sector financiero y pueden extenderse a otros sectores y más allá de las fronteras geográficas. Tienen el potencial de dar lugar a una crisis sistémica, en la que la confianza en el sistema financiero se vea erosionada debido a la perturbación de las funciones que dan apoyo a la economía real, o a pérdidas financieras sustanciosas, alcanzando un nivel que el sistema financiero no pueda soportar o que requiera el despliegue de medidas importantes de amortiguación de choques. Para evitar que se produzcan estos escenarios, que ponen en peligro la estabilidad financiera y la integridad de la Unión, es fundamental lograr la convergencia de las prácticas de supervisión sobre los riesgos relacionados con las TIC derivados de terceros en el sector financiero, en particular mediante nuevas normas que permitan la supervisión por parte de la Unión de los proveedores terceros esenciales de servicios de TIC.

(80) El marco de supervisión depende en gran medida del grado de colaboración entre el supervisor principal y el proveedor tercero esencial de servicios de TIC que presta a entidades financieras servicios que afectan a la prestación de servicios financieros. El éxito de la supervisión depende, entre otras cosas, de la capacidad del supervisor principal para llevar a cabo efectivamente misiones e inspecciones de seguimiento a fin de evaluar las normas, los controles y los procesos utilizados por los proveedores terceros esenciales de servicios de TIC, así como para evaluar el posible efecto acumulado de sus actividades en la estabilidad financiera y la integridad del sistema financiero. Al mismo tiempo, es fundamental que los proveedores terceros esenciales de servicios de TIC sigan las recomendaciones del supervisor principal y atiendan sus preocupaciones. Dado que una falta de cooperación por parte de un proveedor tercero esencial de servicios de TIC que preste servicios que afecten a la prestación de servicios financieros, como la negativa a conceder acceso a sus locales o a facilitar información, privaría en definitiva al supervisor principal de sus herramientas esenciales para evaluar el riesgo relacionado con las TIC derivado de terceros y podría afectar negativamente a la estabilidad financiera y a la integridad del sistema financiero, es necesario también establecer un régimen sancionador acorde.

(81) En este contexto, la necesidad de que el supervisor principal imponga multas coercitivas para obligar a los proveedores terceros esenciales de servicios de TIC a cumplir las obligaciones en materia de transparencia y acceso establecidas en el presente Reglamento no debe verse comprometida por las dificultades planteadas por la ejecución de dichas multas coercitivas en relación con los proveedores terceros esenciales de servicios de TIC establecidos en terceros países. A fin de garantizar que puedan ejecutarse dichas multas y que se implanten rápidamente procedimientos que respeten los derechos de defensa de los proveedores terceros esenciales de servicios de TIC en el contexto del mecanismo de designación y la formulación de recomendaciones, debe exigirse a dichos proveedores terceros esenciales de servicios de TIC que prestan servicios a entidades financieras que afectan a la prestación de servicios financieros que mantengan una presencia empresarial adecuada en la Unión. Debido a la naturaleza de la supervisión y a la ausencia de mecanismos comparables en otros países o territorios, no existe ningún otro mecanismo adecuado que garantice este objetivo mediante una cooperación eficaz con los supervisores financieros de terceros países en lo relativo al seguimiento de la repercusión de los riesgos operativos digitales planteados por proveedores terceros sistémicos de servicios de TIC considerados proveedores terceros esenciales de servicios de TIC establecidos en terceros países. Por tanto, para continuar prestando servicios de TIC a las entidades financieras en la Unión, un proveedor tercero de servicios de TIC establecido en un tercer país designado como esencial con arreglo al presente Reglamento debe tomar, en un plazo de 12 meses a partir de dicha designación, todas las medidas necesarias para garantizar su constitución como sociedad en la Unión mediante el establecimiento de una empresa filial, tal como se define en todo el acervo de la Unión, en concreto en la Directiva 2013/34/UE del Parlamento Europeo y del Consejo ([21]).

(82) El requisito de establecer una empresa filial en la Unión no debe impedir que el proveedor tercero esencial de servicios de TIC preste servicios de TIC y asistencia técnica relacionada con estos desde instalaciones e infraestructuras situadas fuera de la Unión. El presente Reglamento no impone una obligación en materia de localización de datos, ya que no exige que el almacenamiento o el tratamiento de los datos se realice en la Unión.

(83) Los proveedores terceros esenciales de servicios de TIC deben poder prestar servicios de TIC desde cualquier lugar del mundo, no deben necesariamente estar ubicados en la Unión ni prestar servicios únicamente desde locales situados en la Unión. Las actividades de supervisión deben llevarse a cabo en primer lugar en locales situados en la Unión e interactuando con entidades situadas en la Unión, incluidas las empresas filiales establecidas por proveedores terceros esenciales de servicios de TIC con arreglo al presente Reglamento. Sin embargo, estas acciones en la Unión podrían ser insuficientes para que el supervisor principal pueda desempeñar plena y eficazmente sus funciones con arreglo al presente Reglamento. El supervisor principal debe, por lo tanto, poder ejercer sus competencias de supervisión pertinentes en terceros países. El ejercicio de dichas competencias en terceros países debe permitir al supervisor principal examinar las instalaciones desde las que el proveedor tercero esencial de servicios de TIC presta o gestiona realmente servicios de TIC o servicios de asistencia técnica, y debe brindarle un conocimiento completo y operativo de la gestión del riesgo relacionado con las TIC del proveedor tercero esencial de servicios de TIC. La posibilidad de que el supervisor principal, como agencia de la Unión, ejerza sus competencias fuera del territorio de la Unión debe estar debidamente enmarcada con las condiciones pertinentes, en particular el consentimiento del proveedor tercero esencial de servicios de TIC de que se trate. Del mismo modo, las autoridades pertinentes del

([21]) Directiva 2013/34/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los estados financieros anuales, los estados financieros consolidados y otros informes afines de ciertos tipos de empresas, por la que se modifica la Directiva 2006/43/CE del Parlamento Europeo y del Consejo y se derogan las Directivas 78/660/CEE y 83/349/CEE del Consejo (DO L 182 de 29.6.2013, p. 19).

tercer país deben ser informadas del ejercicio en su propio territorio de las actividades del supervisor principal y no deben haberse opuesto a ello. No obstante, para garantizar una aplicación eficaz, y sin perjuicio de las potestades respectivas de las instituciones de la Unión y de los Estados miembros, dichas competencias también deben estar firmemente establecidas mediante la celebración de acuerdos de cooperación administrativa con las autoridades pertinentes del tercer país de que se trate. Por tanto, el presente Reglamento debe permitir a las Autoridades Europeas de Supervisión celebrar acuerdos de cooperación administrativa con las autoridades pertinentes de terceros países que no deben crear de ningún otro modo obligaciones jurídicas con respecto a la Unión y sus Estados miembros.

(84) A fin de facilitar la comunicación con el supervisor principal y garantizar una representación adecuada, los proveedores terceros esenciales de servicios de TIC que formen parte de un grupo deben designar a una persona jurídica como su punto de coordinación.

(85) El marco de supervisión debe entenderse sin perjuicio de la potestad de los Estados miembros para llevar a cabo sus propias misiones de supervisión o seguimiento con respecto a los proveedores terceros de servicios de TIC no designados como esenciales con arreglo al presente Reglamento, pero considerados importantes a escala nacional.

(86) Para aprovechar la arquitectura institucional de múltiples niveles en el ámbito de los servicios financieros, el Comité Mixto de las Autoridades Europeas de Supervisión debe seguir garantizando la coordinación intersectorial general en relación con todos los asuntos relativos al riesgo relacionado con las TIC, de conformidad con sus funciones en materia de ciberseguridad. Debe contar con el apoyo de un nuevo subcomité (Foro de Supervisión) que lleve a cabo trabajos preparatorios tanto para decisiones particulares dirigidas a proveedores terceros esenciales de servicios de TIC como para la formulación de recomendaciones colectivas, en particular en relación con la evaluación comparativa de los programas de supervisión de proveedores terceros esenciales de servicios de TIC, y que determine las buenas prácticas para abordar las cuestiones relativas al riesgo de concentración de TIC.

(87) A fin de garantizar que los proveedores terceros esenciales de servicios de TIC sean objeto de una supervisión apropiada y efectiva a escala de la Unión el presente Reglamento establece que cualquiera de las tres Autoridades Europeas de Supervisión podría ser designada como supervisor principal. La asignación particular de un proveedor tercero esencial de servicios de TIC a una de las tres Autoridades Europeas de Supervisión debe ser el resultado de una evaluación de la preponderancia de las entidades financieras que operan en los sectores financieros sobre los que dicha Autoridad Europea de Supervisión tiene responsabilidades. Este enfoque debe conducir a una distribución equilibrada de tareas y responsabilidades entre las tres Autoridades Europeas de Supervisión en el contexto del ejercicio de las funciones de supervisión y debe hacer el mejor uso posible de los recursos humanos y los conocimientos técnicos especializados disponibles en cada una de ellas.

(88) Deben otorgarse a los supervisores principales las competencias necesarias para llevar a cabo investigaciones, para realizar inspecciones *in situ* y fuera de locales y ubicaciones de proveedores terceros esenciales de servicios de TIC, y para obtener información completa y actualizada. Dichas competencias deben permitir al supervisor principal hacerse una idea precisa del tipo, la dimensión y la repercusión del riesgo relacionado con las TIC derivado de terceros al que se enfrentan las entidades financieras y, en última instancia, el sistema financiero de la Unión. Encomendar a las Autoridades Europeas de Supervisión la función de supervisión principal es un requisito indispensable para comprender y abordar la dimensión sistémica del riesgo relacionado con las TIC en el ámbito financiero. La repercusión de los proveedores terceros esenciales de servicios de TIC en el sector financiero y los problemas que puede ocasionar el consiguiente riesgo de concentración de TIC exigen un enfoque colectivo aplicado a escala de la Unión. El ejercicio simultáneo de varios derechos de acceso y auditorías, desarrollado por separado por numerosas autoridades competentes con una coordinación escasa o nula, impediría a los supervisores financieros obtener una visión general completa y exhaustiva del riesgo relacionado con las TIC derivado de terceros en la Unión, al tiempo que también crearía redundancias, cargas y complejidad para los proveedores terceros esenciales de servicios de TIC en caso de ser objeto de numerosas solicitudes de seguimiento e inspección.

(89) Debido a la importante repercusión que tiene la designación como esencial, el presente Reglamento debe garantizar que los derechos de los proveedores terceros esenciales de servicios de TIC se respeten en toda la aplicación del marco de supervisión. Antes de ser designados como esenciales, dichos proveedores deben, por ejemplo, tener derecho a presentar al supervisor principal una declaración motivada que contenga cualquier información pertinente a efectos de la evaluación relacionada con esa designación. Dado que el supervisor principal debe estar facultado para presentar recomendaciones sobre cuestiones relativas al riesgo relacionado con las TIC y medidas correctoras adecuadas, entre ellas la potestad de oponerse a determinados acuerdos contractuales que afecten en última instancia a la estabilidad de la entidad financiera o del sistema financiero, debe darse asimismo a los proveedores terceros esenciales de servicios de TIC la oportunidad de presentar, antes de ultimar dichas

recomendaciones, explicaciones sobre el efecto esperado de las soluciones previstas en las recomendaciones para los clientes que sean entidades excluidas en el ámbito de aplicación del presente Reglamento, así como de plantear soluciones para mitigar los riesgos. Los proveedores terceros esenciales de servicios de TIC que no estén de acuerdo con las recomendaciones también deben presentar una explicación razonada de su intención de no refrendar la recomendación. Si dicha explicación razonada no se presenta o se considera insuficiente, el supervisor principal debe publicar un aviso en el que se describa brevemente el incumplimiento.

(90) Las autoridades competentes deben incluir debidamente la tarea de verificar el cumplimiento material de las recomendaciones formuladas por el supervisor principal entre sus funciones en relación con la supervisión prudencial de las entidades financieras. Las autoridades competentes deben poder exigir a las entidades financieras que adopten medidas adicionales para hacer frente a los riesgos señalados en las recomendaciones del supervisor principal y, a su debido tiempo, deben emitir notificaciones a tal efecto. Cuando el supervisor principal dirija recomendaciones a proveedores terceros esenciales de servicios de TIC supervisados con arreglo a la Directiva (UE) 2022/2555, las autoridades competentes deben poder consultar, de forma voluntaria y antes de adoptar medidas adicionales, a las autoridades competentes con arreglo a dicha Directiva a fin de propiciar un enfoque coordinado con respecto al tratamiento de los proveedores terceros esenciales de servicios de TIC en cuestión.

(91) El ejercicio de la supervisión debe guiarse por tres principios operativos que buscan garantizar: a) una estrecha coordinación entre las Autoridades Europeas de Supervisión en sus funciones de supervisor principal, mediante una Red de Supervisión Conjunta; b) la coherencia con el marco establecido por la Directiva (UE) 2022/2555 (mediante una consulta voluntaria de los organismos con arreglo a dicha Directiva para evitar la duplicación de las medidas dirigidas a proveedores terceros esenciales de servicios de TIC), y c) la aplicación de medidas de diligencia para reducir al mínimo el posible riesgo de perturbación de los servicios prestados por los proveedores terceros esenciales de servicios de TIC a clientes que sean entidades excluidas del ámbito de aplicación del presente Reglamento.

(92) El marco de supervisión no debe sustituir, en modo alguno ni en ninguna parte, al requisito de que las entidades financieras gestionen ellas mismas los riesgos que entraña el recurso a proveedores terceros de servicios de TIC, incluida la obligación de mantener un seguimiento permanente de los acuerdos contractuales celebrados con proveedores terceros esenciales de servicios de TIC. Asimismo, el marco de supervisión no debe afectar a la plena responsabilidad de las entidades financieras en el cumplimiento y la liberación de todas las obligaciones establecidas en el presente Reglamento y en el Derecho aplicable en materia de servicios financieros.

(93) Para evitar duplicaciones y solapamientos, las autoridades competentes deben abstenerse de adoptar a título particular cualquier medida destinada a hacer un seguimiento de los riesgos de los proveedores terceros esenciales de servicios de TIC y, a ese respecto, deben basarse en la evaluación del supervisor principal correspondiente. Toda medida debe, en cualquier caso, coordinarse y acordarse previamente con el supervisor principal en el contexto de la ejecución de las tareas en el marco de supervisión.

(94) A fin de promover la convergencia a nivel internacional por cuanto se refiere al recurso a las buenas prácticas en la revisión y el seguimiento de la gestión de riesgos digitales por parte de proveedores terceros de servicios de TIC, debe alentarse a las Autoridades Europeas de Supervisión a que celebren acuerdos de cooperación con las autoridades pertinentes de terceros países en materia de supervisión y regulación.

(95) Para aprovechar las competencias, capacidades técnicas y conocimientos específicos del personal especializado en riesgos operativos y relacionados con las TIC de las autoridades competentes, las tres Autoridades Europeas de Supervisión y, a título voluntario, las autoridades competentes con arreglo a la Directiva (UE) 2022/2555, el supervisor principal debe servirse de las capacidades y conocimientos nacionales en materia de supervisión y crear equipos de examinadores para cada proveedor tercero esencial de servicios de TIC, agrupando equipos multidisciplinares para apoyar tanto la preparación como la ejecución de las actividades de supervisión, incluidas las investigaciones generales y las inspecciones de proveedores terceros esenciales de servicios de TIC, así como para cualquier seguimiento que sea necesario.

(96) Mientras que los costes derivados de las tareas de supervisión se financiarían íntegramente con las tasas cobradas a los proveedores terceros esenciales de servicios de TIC, es probable, sin embargo, que las Autoridades Europeas de Supervisión incurran, antes del inicio del marco de supervisión, en gastos para la implantación de sistemas de TIC específicos en apoyo a la próxima supervisión, ya que sería necesario desarrollar y poner en marcha de antemano sistemas de TIC específicos. Por lo tanto, el presente Reglamento establece un modelo de financiación híbrido, en virtud del cual el marco de supervisión como tal se financiaría íntegramente con las tasas, mientras que el desarrollo de los sistemas de TIC de las Autoridades Europeas de Supervisión se financiaría con las contribuciones de la Unión y de las autoridades nacionales competentes.

(97) Las autoridades competentes deben disponer de todas las competencias en materia de supervisión, investigación y sanción requeridas para garantizar el correcto ejercicio de sus obligaciones con arreglo al presente Reglamento. En principio, deben publicar los anuncios de las sanciones administrativas que impongan. Dado que las entidades financieras y los proveedores terceros de servicios de TIC pueden estar establecidos en diferentes Estados miembros y ser controlados por diferentes autoridades competentes, la aplicación del presente Reglamento debe facilitarse, por una parte, mediante una estrecha cooperación entre las autoridades competentes pertinentes, incluido el BCE en relación con las tareas específicas que le encomienda el Reglamento (UE) n.º 1024/2013, y, por otra parte, mediante la consulta con las Autoridades Europeas de Supervisión a través del intercambio recíproco de información y la prestación de asistencia en el contexto de las actividades de control pertinentes.

(98) A fin de cuantificar y calificar en mayor medida los criterios de designación a proveedores terceros de servicios de TIC como esenciales y de armonizar las tasas de supervisión, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE para completar el presente Reglamento mediante una mayor especificación de la repercusión sistémica que un fallo o una interrupción operativa de un proveedor tercero de servicios de TIC podría tener en las entidades financieras a las que presta servicios de TIC, el número de entidades de importancia sistémica mundial (EISM) u otras entidades de importancia sistémica (OEIS) que dependen del proveedor tercero de servicios de TIC correspondiente, el número de proveedores terceros de servicios de TIC activos en un mercado dado, los costes de migración de datos y cargas de trabajo de TIC a otros proveedores terceros de servicios de TIC, así como la cuantía de las tasas de supervisión y las modalidades de pago. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, también a nivel de 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 deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos deben tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(99) Debe garantizarse una armonización coherente de los requisitos establecidos en el presente Reglamento mediante normas técnicas de regulación. Como parte de su función como organismos dotados de conocimientos altamente especializados, las Autoridades Europeas de Supervisión deben elaborar proyectos de normas técnicas de regulación que no conlleven opciones estratégicas, para su presentación a la Comisión. Deben elaborarse normas técnicas de regulación en los ámbitos de la gestión del riesgo relacionado con las TIC, la notificación de incidentes graves relacionados con las TIC, la realización de pruebas, así como en lo relativo a los requisitos clave para un seguimiento adecuado del riesgo relacionado con las TIC derivado de terceros. La Comisión y las Autoridades Europeas de Supervisión deben garantizar que todas las entidades financieras puedan aplicar esas normas y esos requisitos de manera proporcionada a su tamaño y perfil de riesgo general, así como a la naturaleza, escala y complejidad de sus servicios, actividades y operaciones. Se deben otorgar a la Comisión poderes para adoptar dichas normas técnicas de regulación mediante actos delegados con arreglo al artículo 290 del TFUE y de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

(100) A fin de facilitar la comparabilidad de las notificaciones sobre incidentes graves relacionados con las TIC e incidentes operativos o de seguridad graves relacionados con los pagos, así como de garantizar la transparencia de los acuerdos contractuales para el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC, las Autoridades Europeas de Supervisión deben elaborar proyectos de normas técnicas de ejecución que establezcan plantillas, formularios y procedimientos normalizados para la notificación por las entidades financieras de incidentes graves relacionados con las TIC y de incidentes graves operativos o de seguridad relacionados con los pagos, así como plantillas normalizadas para el registro de información. A la hora de elaborar dichas normas, las Autoridades Europeas de Supervisión deben tener en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones. Deben conferirse a la Comisión competencias para adoptar dichas normas técnicas de ejecución mediante actos de ejecución con arreglo al artículo 291 del TFUE y de conformidad con el artículo 15 del Reglamento (UE) n.º 1093/2010, el artículo 15 del Reglamento (UE) n.º 1094/2010 y el artículo 15 del Reglamento (UE) n.º 1095/2010.

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

(101) Dado que ya se han especificado requisitos adicionales mediante actos delegados y de ejecución basados en normas técnicas de regulación y de ejecución en virtud de los Reglamentos (CE) n.º 1060/2009 ([23]), (UE) n.º 648/2012 ([24]), (UE) n.º 600/2014 ([25]) y (UE) n.º 909/2014 ([26]) del Parlamento Europeo y del Consejo, procede encomendar a las Autoridades Europeas de Supervisión que presenten a la Comisión, ya sea a título particular o conjuntamente a través del Comité Mixto, normas técnicas de regulación y de ejecución para la adopción de actos delegados y de ejecución que incorporen y actualicen las actuales normas de gestión del riesgo relacionado con las TIC.

(102) Dado que el presente Reglamento, junto con la Directiva (UE) 2022/2556 del Parlamento Europeo y del Consejo ([27]), implica una consolidación de las disposiciones en materia de gestión del riesgo relacionado con las TIC de varios reglamentos y directivas del acervo de la Unión sobre servicios financieros, incluidos los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014 y el Reglamento (UE) 2016/1011 del Parlamento Europeo y del Consejo ([28]), con el fin de garantizar la plena coherencia se deben modificar dichos Reglamentos para aclarar que el presente Reglamento establece las disposiciones aplicables en materia de riesgo relacionado con las TIC.

(103) Por consiguiente, debe delimitarse el ámbito de aplicación de los artículos pertinentes relacionados con el riesgo operativo en virtud de los cuales se encomendaban la adopción de actos delegados y de ejecución en las habilitaciones establecidas en 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, con el fin de incorporar al presente Reglamento todas las disposiciones relativas a los aspectos de la resiliencia operativa digital que forman actualmente parte de dichos Reglamentos.

(104) El posible riesgo de ciberseguridad sistémico asociado al uso de infraestructuras de TIC que permiten el funcionamiento de los sistemas de pago y la realización de actividades de procesamiento de pagos debe abordarse debidamente a escala de la Unión mediante normas armonizadas en materia de resiliencia digital. A tal efecto, la Comisión debe evaluar rápidamente la necesidad de revisar el ámbito de aplicación del presente Reglamento, ajustando al mismo tiempo dicha revisión al resultado de la evaluación completa que se contempla con arreglo a la Directiva (UE) 2015/2366. Numerosos ataques a gran escala durante el último decenio demuestran hasta qué punto los sistemas de pago han quedado expuestos a ciberamenazas. Situados en el centro de la cadena de servicios de pago e interconectados firmemente con el sistema financiero general, los sistemas de pago y las actividades de procesamiento de pagos han adquirido una importancia crucial para el funcionamiento de los mercados financieros de la Unión. Los ciberataques a estos sistemas pueden provocar perturbaciones graves de la actividad con repercusiones directas en funciones económicas clave, como la facilitación de los pagos, y efectos indirectos en los procesos económicos conexos. Hasta que se establezcan a escala de la Unión un régimen armonizado y la supervisión de los operadores de sistemas de pago y entidades de procesamiento, los Estados miembros, con vistas a aplicar prácticas de mercado similares, podrán inspirarse en los requisitos de resiliencia operativa digital establecidos en el presente Reglamento al aplicar normas a los operadores de sistemas de pago y a las entidades de procesamiento controlados en sus propias jurisdicciones.

([23]) Reglamento (CE) n.º 1060/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre las agencias de calificación crediticia (DO L 302 de 17.11.2009, p. 1).

([24]) 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).

([25]) Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 173 de 12.6.2014, p. 84).

([26]) Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la mejora de la liquidación de valores en la Unión Europea y los depositarios centrales de valores y por el que se modifican las Directivas 98/26/CE y 2014/65/UE y el Reglamento (UE) n.º 236/2012 (DO L 257 de 28.8.2014, p. 1).

([27]) Directiva (UE) 2022/2556 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se modifican las Directivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 en lo relativo a la resiliencia operativa digital del sector financiero (véase la página 153 del presente Diario Oficial).

([28]) Reglamento (UE) 2016/1011 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, sobre los índices utilizados como referencia en los instrumentos financieros y en los contratos financieros o para medir la rentabilidad de los fondos de inversión, y por el que se modifican las Directivas 2008/48/CE y 2014/17/UE y el Reglamento (UE) n.º 596/2014 (DO L 171 de 29.6.2016, p. 1).

(105) Dado que el objetivo del presente Reglamento, a saber, conseguir un alto nivel de resiliencia operativa digital para las entidades financieras reguladas, no puede ser alcanzado de manera suficiente por los Estados miembros, pues requiere la armonización de algunas normas diferentes del Derecho de la Unión y nacional, sino que, debido a su dimensión y efectos, puede alcanzarse mejor a escala de la Unión, esta última 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 ese mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(106) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([29]), emitió su dictamen el 10 de mayo de 2021 ([30]).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

Disposiciones generales

Artículo 1

Objeto

1. A fin de lograr un elevado nivel común de resiliencia operativa digital, el presente Reglamento establece requisitos uniformes relativos a la seguridad de las redes y los sistemas de información que sustentan los procesos empresariales de las entidades financieras como sigue:

a) requisitos aplicables a las entidades financieras en relación con:

   i) la gestión del riesgo en el ámbito de las tecnologías de la información y la comunicación (TIC),

   ii) la notificación a las autoridades competentes de incidentes graves relacionados con las TIC y, con carácter voluntario, de ciberamenazas importantes,

   iii) la notificación a las autoridades competentes de incidentes operativos o de seguridad graves relacionados con los pagos por parte de las entidades financieras a las que se hace referencia en el artículo 2, apartado 1, letras a) a d),

   iv) las pruebas de resiliencia operativa digital,

   v) el intercambio de información e inteligencia en relación con las ciberamenazas y las vulnerabilidades cibernéticas,

   vi) las medidas para la buena gestión del riesgo relacionado con las TIC derivado de terceros;

b) requisitos en relación con los acuerdos contractuales celebrados entre proveedores terceros de servicios de TIC y entidades financieras;

c) normas para el establecimiento y aplicación del marco de supervisión de los proveedores terceros esenciales de servicios de TIC cuando presten servicios a entidades financieras;

d) normas sobre cooperación entre autoridades competentes y normas sobre control y ejecución por parte de las autoridades competentes en relación con todos los asuntos cubiertos por el presente Reglamento.

2. En relación con las entidades financieras identificadas como entidades esenciales o importantes en virtud de las normas nacionales de transposición del artículo 3 de la Directiva (UE) 2022/2555, el presente Reglamento se considerará un acto jurídico sectorial de la Unión a efectos del artículo 4 de dicha Directiva.

3. El presente Reglamento se entenderá sin perjuicio de la responsabilidad de los Estados miembros en lo concerniente a las funciones esenciales del Estado que afectan a la seguridad pública, la defensa y la seguridad nacional de conformidad con el Derecho de la Unión.

([29]) 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).

([30]) DO C 229 de 15.6.2021, p. 16.

Artículo 2

Ámbito de aplicación

1. Sin perjuicio de lo dispuesto en los apartados 3 y 4, el presente Reglamento se aplicará a las siguientes entidades:

a) entidades de crédito;

b) entidades de pago, incluidas las entidades de pago exentas en virtud de la Directiva (UE) 2015/2366;

c) proveedores de servicios de información sobre cuentas;

d) entidades de dinero electrónico, incluidas las entidades de dinero electrónico exentas en virtud de la Directiva 2009/110/CE;

e) empresas de servicios de inversión;

f) proveedores de servicios de criptoactivos autorizados en virtud de un Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 (en lo sucesivo, «Reglamento relativo a los mercados de criptoactivos»), y emisores de fichas referenciadas a activos;

g) depositarios centrales de valores;

h) entidades de contrapartida central;

i) centros de negociación;

j) registros de operaciones;

k) gestores de fondos de inversión alternativos;

l) sociedades de gestión;

m) proveedores de servicios de suministro de datos;

n) empresas de seguros y de reaseguros;

o) intermediarios de seguros, intermediarios de reaseguros e intermediarios de seguros complementarios;

p) fondos de pensiones de empleo;

q) agencias de calificación crediticia;

r) administradores de índices de referencia cruciales;

s) proveedores de servicios de financiación participativa;

t) registros de titulizaciones;

u) proveedores terceros de servicios de TIC.

2. A efectos del presente Reglamento, las entidades a que se refiere el apartado 1, letras a) a t), se denominarán colectivamente «entidades financieras».

3. El presente Reglamento no se aplicará a:

a) los gestores de fondos de inversión alternativos tal como se contemplan en el artículo 3, apartado 2, de la Directiva 2011/61/UE;

b) las empresas de seguros y de reaseguros tal como se contemplan en el artículo 4 de la Directiva 2009/138/CE;

c) los fondos de pensiones de empleo que gestionen planes de pensiones que, en conjunto, no tengan más de quince partícipes en total;

d) las personas físicas o jurídicas exentas en virtud de los artículos 2 y 3 de la Directiva 2014/65/UE;

e) los intermediarios de seguros, los intermediarios de reaseguros y los intermediarios de seguros complementarios que sean microempresas o pequeñas o medianas empresas;

f) las oficinas de cheques postales tal como se contemplan en el artículo 2, apartado 5, punto 3, de la Directiva 2013/36/UE.

4. Los Estados miembros podrán excluir del ámbito de aplicación del presente Reglamento a las entidades a que se refiere el artículo 2, apartado 5, puntos 4 a 23, de la Directiva 2013/36/UE que estén situadas en sus respectivos territorios. Cuando un Estado miembro haga uso de esta posibilidad, informará de ello a la Comisión, así como de cualquier modificación posterior al respecto. La Comisión hará pública esta información en su sitio web o por otros medios fácilmente accesibles.

Artículo 3

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «resiliencia operativa digital»: la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones;

2) «red y sistema de información»: una red y un sistema de información según se definen en el artículo 6, punto 1, de la Directiva (UE) 2022/2555;

3) «sistema de TIC heredado»: un sistema de TIC que ha alcanzado el final de su ciclo de vida (final de vida útil) y que por razones tecnológicas o comerciales no admite actualizaciones o correcciones, o para el que su proveedor o un proveedor tercero de servicios de TIC ya no presta asistencia técnica, pero que sigue utilizándose y sustenta las funciones de la entidad financiera;

4) «seguridad de las redes y sistemas de información»: la seguridad de las redes y sistemas de información según se define en el artículo 6, punto 2, de la Directiva (UE) 2022/2555;

5) «riesgo relacionado con las TIC»: cualquier circunstancia razonablemente identificable en relación con el uso de redes y sistemas de información que, si se materializa, puede comprometer la seguridad de las redes y sistemas de información, de cualquier herramienta o proceso dependiente de la tecnología, de las operaciones y los procesos o de la prestación de servicios, al provocar efectos adversos en el entorno digital o físico;

6) «activo de información»: un compendio de información, tangible o intangible, que conviene proteger;

7) «activo de TIC»: un activo de *software* o *hardware* en las redes y sistemas de información utilizados por la entidad financiera;

8) «incidente relacionado con las TIC»: un único suceso o una serie de sucesos interrelacionados no previstos por la entidad financiera que pone en peligro la seguridad de las redes y sistemas de información y tiene repercusiones negativas en la disponibilidad, autenticidad, integridad o confidencialidad de los datos o en los servicios prestados por la entidad financiera;

9) «incidente operativo o de seguridad relacionado con los pagos»: un único suceso o una serie de sucesos interrelacionados no previstos por las entidades financieras a que se refiere el artículo 2, apartado 1, letras a) a d), estén o no relacionados con las TIC, que tiene repercusiones negativas en la confidencialidad, disponibilidad, integridad o autenticidad de los datos relacionados con los pagos o en los servicios relacionados con los pagos prestados por la entidad financiera;

10) «incidente grave relacionado con las TIC»: un incidente relacionado con las TIC con graves repercusiones negativas en las redes y sistemas de información que sustentan funciones esenciales o importantes de la entidad financiera;

11) «incidente operativo o de seguridad grave relacionado con los pagos»: un incidente operativo o de seguridad relacionado con los pagos con graves repercusiones negativas en los servicios relacionados con los pagos prestados;

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

13) «ciberamenaza importante»: una ciberamenaza cuyas características técnicas indican que podría dar lugar a un incidente grave relacionado con las TIC o a un incidente operativo o de seguridad grave relacionado con los pagos;

14) «ciberataque»: un incidente malintencionado relacionado con las TIC provocado mediante una tentativa, perpetrada por cualquier agente de riesgo, de destruir, revelar, alterar, desactivar o robar un activo, de obtener acceso no autorizado a ese activo o de hacer uso no autorizado de él;

15) «inteligencia sobre amenazas»: información que se ha agregado, transformado, analizado, interpretado o enriquecido para proporcionar el contexto necesario para la toma de decisiones y permitir una comprensión pertinente y suficiente para mitigar las repercusiones de un incidente relacionado con las TIC o de una ciberamenaza, incluidos los detalles técnicos de un ciberataque, los responsables del ataque, su *modus operandi* y sus motivaciones;

16) «vulnerabilidad»: una debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado;

17) «pruebas de penetración basadas en amenazas»: un marco que imita las tácticas, técnicas y procedimientos de agentes de amenazas reales que se considera presentan una auténtica ciberamenaza, que permite someter a prueba (equipo rojo) de forma controlada, a medida y en función de la inteligencia los sistemas de producción activos esenciales de la entidad financiera;

18) «riesgo relacionado con las TIC derivado de terceros»: el riesgo relacionado con las TIC al que puede verse expuesta una entidad financiera en razón de su uso de servicios de TIC prestados por proveedores terceros de servicios de TIC o por subcontratistas de estos últimos, a través, entre otros, de acuerdos de externalización;

19) «proveedor tercero de servicios de TIC»: una empresa que presta servicios de TIC;

20) «proveedor intragrupo de servicios de TIC»: una empresa que forma parte de un grupo financiero y presta principalmente servicios de TIC a entidades financieras del mismo grupo o a entidades financieras que pertenecen al mismo sistema institucional de protección, también a sus sociedades matrices, filiales o sucursales o a otras entidades que compartan propiedad o control;

21) «servicios de TIC»: los servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua, incluidos el *hardware* como servicio y los servicios de *hardware* que incluyen la prestación de asistencia técnica a través de actualizaciones de *software* o *firmware* por parte del proveedor de *hardware* y excluidos los servicios telefónicos analógicos tradicionales;

22) «función esencial o importante»: una función cuya perturbación afectaría significativamente al rendimiento financiero de una entidad financiera o a la solidez o continuidad de sus servicios y actividades o cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización, o con sus demás obligaciones con arreglo al Derecho aplicable en materia de servicios financieros;

23) «proveedor tercero esencial de servicios de TIC»: un proveedor tercero de servicios de TIC designado como esencial de conformidad con el artículo 31;

24) «proveedor tercero de servicios de TIC establecido en un tercer país»: un proveedor tercero de servicios de TIC que sea una persona jurídica establecida en un tercer país que haya celebrado un acuerdo contractual con una entidad financiera para la prestación de servicios de TIC;

25) «filial»: una empresa filial en el sentido del artículo 2, punto 10, y del artículo 22 de la Directiva 2013/34/UE;

26) «grupo»: un grupo tal como se define en el artículo 2, punto 11, de la Directiva 2013/34/UE;

27) «sociedad matriz»: una sociedad matriz en el sentido del artículo 2, punto 9, y del artículo 22 de la Directiva 2013/34/UE;

28) «subcontratista de TIC establecido en un tercer país»: un subcontratista de TIC que sea una persona jurídica establecida en un tercer país y que haya celebrado un acuerdo contractual con un proveedor tercero de servicios de TIC o con un proveedor tercero de servicios de TIC establecido en un tercer país;

29) «riesgo de concentración de TIC»: una exposición a uno o múltiples proveedores terceros esenciales de servicios de TIC relacionados que cree tal grado de dependencia de dichos proveedores que la indisponibilidad, fallo u otro tipo de deficiencia de estos últimos pueda poner en peligro la capacidad de una entidad financiera para desempeñar funciones esenciales o importantes o causarle otro tipo de efectos adversos, incluidas grandes pérdidas, o poner en peligro la estabilidad financiera de la Unión en su conjunto;

30) «órgano de dirección»: un órgano de dirección tal como se define en el artículo 4, apartado 1, punto 36, de la Directiva 2014/65/UE, el artículo 3, apartado 1, punto 7, de la Directiva 2013/36/UE, el artículo 2, apartado 1, letra s), de la Directiva 2009/65/CE del Parlamento Europeo y del Consejo ([31]), el artículo 2, apartado 1, punto 45, del Reglamento (UE) n.º 909/2014, el artículo 3, apartado 1, punto 20, del Reglamento (UE) 2016/1011 y las disposiciones pertinentes del Reglamento relativo a los mercados de criptoactivos, o las personas equivalentes que dirijan efectivamente la entidad o desempeñen funciones clave de conformidad con el Derecho de la Unión o nacional pertinente;

31) «entidad de crédito»: una entidad de crédito tal como se define en el artículo 4, apartado 1, punto 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([32]);

32) «entidad exenta en virtud de la Directiva 2013/36/UE»: una entidad a que se refiere el artículo 2, apartado 5, puntos 4 a 23, de la Directiva 2013/36/UE;

33) «empresa de servicios de inversión»: una empresa de servicios de inversión tal como se define en el artículo 4, apartado 1, punto 1, de la Directiva 2014/65/UE;

34) «empresa de servicios de inversión pequeña y no interconectada»: una empresa de servicios de inversión que cumple las condiciones establecidas en el artículo 12, apartado 1, del Reglamento (UE) 2019/2033 del Parlamento Europeo y del Consejo ([33]);

35) «entidad de pago»: una entidad de pago tal como se define en el artículo 4, punto 4, de la Directiva (UE) 2015/2366;

36) «entidad de pago exenta en virtud de la Directiva (UE) 2015/2366»: una entidad de pago exenta en virtud del artículo 32, apartado 1, de la Directiva (UE) 2015/2366;

37) «proveedor de servicios de información sobre cuentas»: un proveedor de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la Directiva (UE) 2015/2366;

38) «entidad de dinero electrónico»: una entidad de dinero electrónico tal como se define en el artículo 2, punto 1, de la Directiva 2009/110/CE;

39) «entidad de dinero electrónico exenta en virtud de la Directiva 2009/110/CE»: una entidad de dinero electrónico que se beneficia de una exención a tenor del artículo 9, apartado 1, de la Directiva 2009/110/CE;

40) «entidad de contrapartida central»: una entidad de contrapartida central tal como se define en el artículo 2, punto 1, del Reglamento (UE) n.º 648/2012;

41) «registro de operaciones»: un registro de operaciones tal como se define en el artículo 2, punto 2, del Reglamento (UE) n.º 648/2012;

42) «depositario central de valores»: un depositario central de valores tal como se define en el artículo 2, apartado 1, punto 1, del Reglamento (UE) n.º 909/2014;

43) «centro de negociación»: un centro de negociación tal como se define en el artículo 4, apartado 1, punto 24, de la Directiva 2014/65/UE;

44) «gestor de fondos de inversión alternativos»: un gestor de fondos de inversión alternativos tal como se define en el artículo 4, apartado 1, letra b), de la Directiva 2011/61/UE;

45) «sociedad de gestión»: una sociedad de gestión tal como se define en el artículo 2, apartado 1, letra b), de la Directiva 2009/65/CE;

46) «proveedor de servicios de suministro de datos»: un proveedor de servicios de suministro de datos en el sentido del Reglamento (UE) n.º 600/2014, a que se refiere su artículo 2, apartado 1, puntos 34 a 36;

47) «empresa de seguros»: una empresa de seguros tal como se define en el artículo 13, punto 1, de la Directiva 2009/138/CE;

48) «empresa de reaseguros»: una empresa de reaseguros tal como se define en el artículo 13, punto 4, de la Directiva 2009/138/CE;

([31]) Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM) (DO L 302 de 17.11.2009, p. 32).

([32]) 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).

([33]) Reglamento (UE) 2019/2033 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativo a los requisitos prudenciales de las empresas de servicios de inversión, y por el que se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 575/2013, (UE) n.º 600/2014 y (UE) n.º 806/2014 (DO L 314 de 5.12.2019, p. 1).

49) «intermediario de seguros»: un intermediario de seguros tal como se define en el artículo 2, apartado 1, punto 3, de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo ([34]);

50) «intermediario de seguros complementarios»: un intermediario de seguros complementarios tal como se define en el artículo 2, apartado 1, punto 4, de la Directiva (UE) 2016/97;

51) «intermediario de reaseguros»: un intermediario de reaseguros tal como se define en el artículo 2, apartado 1, punto 5, de la Directiva (UE) 2016/97;

52) «fondo de pensiones de empleo»: un fondo de pensiones de empleo tal como se define en el artículo 6, punto 1, de la Directiva (UE) 2016/2341;

53) «fondo de pensiones de empleo pequeño»: un fondo de pensiones de empleo que gestiona planes de pensiones que cuentan con menos de 100 partícipes en total;

54) «agencia de calificación crediticia»: una agencia de calificación crediticia tal como se define en el artículo 3, apartado 1, letra b), del Reglamento (CE) n.º 1060/2009;

55) «proveedor de servicios de criptoactivos»: un proveedor de servicios de criptoactivos tal como se define en las disposiciones pertinentes del Reglamento relativo a los mercados de criptoactivos;

56) «emisor de fichas referenciadas a activos»: un emisor de fichas referenciadas a activos tal como se definen en las disposiciones pertinentes del Reglamento relativo a los mercados de criptoactivos;

57) «administrador de índices de referencia cruciales»: un administrador de «índices de referencia cruciales» tal como se definen en el artículo 3, apartado 1, punto 25, del Reglamento (UE) 2016/1011;

58) «proveedor de servicios de financiación participativa»: un proveedor de servicios de financiación participativa tal como se define en el artículo 2, apartado 1, letra e), del Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo ([35]);

59) «registro de titulizaciones»: un registro de titulizaciones tal como se define en el artículo 2, punto 23, del Reglamento (UE) 2017/2402 del Parlamento Europeo y del Consejo ([36]);

60) «microempresa»: una entidad financiera distinta de un centro de negociación, una entidad de contrapartida central, un registro de operaciones o un depositario central de valores, que emplea a menos de diez personas y cuyo volumen de negocios anual o balance anual total es igual o inferior a 2 millones EUR;

61) «supervisor principal»: la Autoridad Europea de Supervisión nombrada de conformidad con el artículo 31, apartado 1, letra b), del presente Reglamento;

62) «Comité Mixto»: el comité a que se refiere el artículo 54 del Reglamento (UE) n.º 1093/2010, el artículo 54 del Reglamento (UE) n.º 1094/2010 y el artículo 54 del Reglamento (UE) n.º 1095/2010;

63) «pequeña empresa»: una entidad financiera que emplea a 10 o más personas pero menos de 50 y cuyo volumen de negocios anual o balance anual total es superior a 2 millones EUR pero igual o inferior a 10 millones EUR;

64) «mediana empresa»: una entidad financiera distinta de una pequeña empresa, que emplea a menos de 250 personas y cuyo volumen de negocios anual es igual o inferior a 50 millones EUR o cuyo balance anual es igual o inferior a 43 millones EUR;

65) «autoridad pública»: cualquier gobierno u otra entidad de la administración pública, incluidos los bancos centrales nacionales.

([34]) Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (DO L 26 de 2.2.2016, p. 19).

([35]) Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas, y por el que se modifican el Reglamento (UE) 2017/1129 y la Directiva (UE) 2019/1937 (DO L 347 de 20.10.2020, p. 1).

([36]) Reglamento (UE) 2017/2402 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2017, por el que se establece un marco general para la titulización y se crea un marco específico para la titulización simple, transparente y normalizada, y por el que se modifican las Directivas 2009/65/CE, 2009/138/CE y 2011/61/UE y los Reglamentos (CE) n.º 1060/2009 y (UE) n.º 648/2012 (DO L 347 de 28.12.2017, p. 35).

Artículo 4

Principio de proporcionalidad

1. Las entidades financieras aplicarán las normas establecidas en el capítulo II de conformidad con el principio de proporcionalidad, teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

2. Además, la aplicación por parte de las entidades financieras de los capítulos III y IV y el capítulo V, sección I, será proporcional a su tamaño y perfil de riesgo general, así como a la naturaleza, escala y complejidad de sus servicios, actividades y operaciones, tal como se establece específicamente en las normas pertinentes de dichos capítulos.

3. Las autoridades competentes tendrán en cuenta la aplicación del principio de proporcionalidad por parte de las entidades financieras al revisar la coherencia del marco de gestión del riesgo relacionado con las TIC a partir de los informes presentados a petición de las autoridades competentes en virtud del artículo 6, apartado 5, y al artículo 16, apartado 2.

CAPÍTULO II

Gestión del riesgo relacionado con las TIC

Sección I

Artículo 5

Gobernanza y organización

1. A fin lograr un nivel elevado de resiliencia operativa digital, las entidades financieras dispondrán de un marco interno de gobernanza y control que garantice una gestión efectiva y prudente del riesgo relacionado con las TIC, de conformidad con el artículo 6, apartado 4.

2. El órgano de dirección de la entidad financiera definirá, aprobará y supervisará todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, y será responsable de su aplicación.

A efectos del párrafo primero, el órgano de dirección:

a) asumirá la responsabilidad última de gestionar el riesgo relacionado con las TIC de la entidad financiera;

b) adoptará políticas encaminadas a garantizar el mantenimiento de unos niveles elevados de disponibilidad, autenticidad, integridad y confidencialidad de los datos;

c) definirá claramente los cometidos y responsabilidades por lo que respecta a todas las funciones relacionadas con las TIC y establecerá mecanismos de gobernanza adecuados para garantizar una comunicación, cooperación y coordinación efectivas y oportunas entre dichas funciones;

d) asumirá la responsabilidad general de establecer y aprobar la estrategia de resiliencia operativa digital a que se refiere el artículo 6, apartado 8, lo que incluye determinar el nivel adecuado de tolerancia al riesgo relacionado con las TIC de la entidad financiera a que se refiere el artículo 6, apartado 8, letra b);

e) aprobará, supervisará y revisará periódicamente la aplicación de la política de continuidad de la actividad en materia de TIC y de los planes de respuesta y recuperación en materia de TIC de la entidad financiera a que se refiere, respectivamente, el artículo 11 apartados 1 y 3, que podrán ser adoptados como una política específica que forme parte integrante de la política global de continuidad de la actividad y del plan de respuesta y recuperación de la entidad financiera;

f) aprobará y revisará periódicamente los planes de auditoría internos de TIC y las auditorías de TIC de la entidad financiera, así como sus modificaciones significativas;

g) asignará y revisará periódicamente el presupuesto adecuado para satisfacer las necesidades de resiliencia operativa digital de la entidad financiera con respecto a todos los tipos de recursos, incluidos los programas de sensibilización en materia de seguridad de las TIC y las actividades de formación sobre resiliencia operativa digital pertinentes a que se refiere el artículo 13, apartado 6, y las capacidades en materia de TIC para todo el personal;

h) aprobará y revisará periódicamente la política de la entidad financiera sobre los acuerdos relativos al uso de servicios de TIC prestados por proveedores terceros de servicios de TIC;

i) establecerá, a escala corporativa, canales de comunicación que le permitan estar debidamente informado de lo siguiente:

   i) de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC,

   ii) de cualquier cambio sustancial pertinente previsto en relación con los proveedores terceros de servicios de TIC,

   iii) de las posibles repercusiones de tales cambios en las funciones esenciales o importantes reguladas por dichos acuerdos, incluido un resumen del análisis de riesgos para evaluar las repercusiones de dichos cambios, y al menos de los incidentes graves relacionados con las TIC y sus repercusiones, así como de las medidas de respuesta, recuperación y corrección.

3. Las entidades financieras que no sean microempresas crearán un cargo para el seguimiento de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC o designarán a un miembro de la alta dirección como responsable de supervisar la exposición al riesgo correspondiente y la documentación pertinente.

4. Los miembros del órgano de dirección de la entidad financiera mantendrán al día de manera activa conocimientos y capacidades suficientes para comprender y evaluar el riesgo relacionado con las TIC y sus repercusiones en las operaciones de la entidad financiera, también siguiendo periódicamente una formación específica que sea acorde al riesgo relacionado con las TIC que se esté gestionando.

Sección II

Artículo 6

Marco de gestión del riesgo relacionado con las TIC

1. Las entidades financieras contarán con un marco de gestión del riesgo relacionado con las TIC sólido, completo y bien documentado como parte de su sistema global de gestión de riesgos, que les permita hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia operativa digital.

2. El marco de gestión del riesgo relacionado con las TIC incluirá al menos las estrategias, las políticas, los procedimientos, y los protocolos y herramientas de TIC que sean necesarios para proteger debida y adecuadamente todos los activos de información y activos de TIC, incluidos el *software*, el *hardware* y los servidores, así como para proteger todos los componentes e infraestructuras físicos pertinentes, como locales, centros de datos y zonas sensibles designadas, a fin de garantizar que todos los activos de información y activos de TIC estén adecuadamente protegidos de los riesgos, incluidos los daños y el acceso o uso no autorizados.

3. De conformidad con el marco de gestión del riesgo relacionado con las TIC, las entidades financieras minimizarán las consecuencias de dicho riesgo mediante el despliegue de estrategias, políticas, procedimientos, protocolos y herramientas de TIC adecuados. Proporcionarán a las autoridades competentes que lo soliciten información completa y actualizada sobre el riesgo relacionado con las TIC y sobre su marco de gestión de dicho riesgo.

4. Las entidades financieras que no sean microempresas encomendarán a una función de control la gestión y la supervisión del riesgo relacionado con las TIC y garantizarán un nivel adecuado de independencia de dicha función para evitar conflictos de intereses. Las entidades financieras garantizarán una separación e independencia adecuadas de las funciones de gestión del riesgo relacionado con las TIC, las funciones de control y las funciones de auditoría interna, con arreglo al modelo de tres líneas de defensa o a un modelo interno de gestión y control de riesgos.

5. El marco de gestión del riesgo relacionado con las TIC se documentará y revisará al menos una vez al año, o periódicamente en el caso de las microempresas, así como cuando se produzcan incidentes graves relacionados con las TIC, y siguiendo las instrucciones de supervisión o conclusiones derivadas de los procesos pertinentes de prueba o auditoría de la resiliencia operativa digital. Se mejorará continuamente sobre la base de las enseñanzas derivadas de la aplicación y el seguimiento. Se presentará a la autoridad competente que lo solicite un informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC.

6. El marco de gestión del riesgo relacionado con las TIC de las entidades financieras que no sean microempresas será objeto de auditoría interna llevada a cabo por auditores con carácter periódico en consonancia con el plan de auditoría de las entidades financieras. Dichos auditores poseerán conocimientos, capacidades y pericia suficientes en materia de riesgo relacionado con las TIC, y gozarán de la independencia adecuada. La frecuencia y el enfoque de las auditorías de TIC serán acordes con el riesgo relacionado con las TIC de la entidad financiera.

7. A partir de las conclusiones de la auditoría interna, las entidades financieras establecerán un proceso formal de seguimiento que incluirá normas para la oportuna verificación y corrección de los resultados problemáticos de la auditoría de TIC.

8. El marco de gestión del riesgo relacionado con las TIC incluirá una estrategia de resiliencia operativa digital que establezca cómo se aplicará el marco. A tal fin, la estrategia de resiliencia operativa digital incluirá métodos para hacer frente al riesgo relacionado con las TIC y alcanzar los objetivos específicos en materia de TIC, para lo cual:

a) explicará cómo apoya el marco de gestión del riesgo relacionado con las TIC la estrategia y los objetivos empresariales de la entidad financiera;

b) establecerá el nivel de tolerancia al riesgo relacionado con las TIC, de acuerdo con la propensión al riesgo de la entidad financiera, y analizará la tolerancia al impacto de las perturbaciones de las TIC;

c) establecerá objetivos claros en materia de seguridad de la información, incluidos indicadores clave de rendimiento y parámetros clave de medición del riesgo;

d) explicará la arquitectura de referencia de TIC y cualquier cambio necesario para alcanzar objetivos empresariales específicos;

e) esbozará los diferentes mecanismos establecidos para detectar incidentes relacionados con las TIC, prevenir su impacto y protegerse de sus efectos;

f) hará constar la situación actual de la resiliencia operativa digital sobre la base del número de incidentes graves relacionados con las TIC notificados y la eficacia de las medidas preventivas;

g) efectuará pruebas de resiliencia operativa digital, de conformidad con el capítulo IV del presente Reglamento;

h) esbozará una estrategia de comunicación en caso de aquellos incidentes relacionados con las TIC que sea obligatorio divulgar conformidad con el artículo 14.

9. Las entidades financieras podrán, en el contexto de la estrategia de resiliencia operativa digital a que se refiere el apartado 8, definir una estrategia global multiproveedor en materia de TIC a nivel de grupo o entidad, que muestre las dependencias clave de los proveedores terceros de servicios de TIC y explique los motivos subyacentes a la contratación de una combinación de proveedores terceros de servicios de TIC.

10. Las entidades financieras podrán externalizar, de conformidad con el Derecho sectorial de la Unión y nacional, a empresas externas o de su mismo grupo las tareas de verificación del cumplimiento de los requisitos de gestión del riesgo relacionado con las TIC. En los casos en que se produzca tal externalización, la entidad financiera seguirá siendo plenamente responsable de la verificación del cumplimiento de los requisitos en materia de gestión del riesgo relacionado con las TIC.

Artículo 7

Sistemas, protocolos y herramientas de TIC

Con el fin de abordar y gestionar los riesgos relacionados con las TIC, las entidades financieras utilizarán y mantendrán actualizados sistemas, protocolos y herramientas de TIC que:

a) sean adecuados a la magnitud de las operaciones que sustentan la realización de sus actividades, de conformidad con el principio de proporcionalidad a que se refiere el artículo 4;

b) sean fiables;

c) dispongan de capacidad suficiente para tratar con exactitud los datos necesarios para llevar a cabo las actividades y prestar los servicios a tiempo, y para hacer frente a los volúmenes máximos de pedidos, mensajes u operaciones, según sea necesario, también en caso de introducción de nuevas tecnologías;

d) sean tecnológicamente resilientes a fin de hacer frente adecuadamente a las necesidades adicionales de tratamiento de la información que surjan en condiciones de tensión del mercado u otras situaciones adversas.

Artículo 8

Identificación

1. Como parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, las entidades financieras identificarán, clasificarán y documentarán adecuadamente todas las funciones, cometidos y responsabilidades empresariales sustentados por las TIC, los activos de información y activos de TIC que sustenten dichas funciones, y sus cometidos y dependencias en relación con el riesgo relacionado con las TIC. Las entidades financieras revisarán en caso necesario, y al menos una vez al año, la idoneidad de esta clasificación y de cualquier documentación pertinente.

2. Las entidades financieras identificarán de forma continua todas las fuentes de riesgo relacionado con las TIC, en particular la exposición al riesgo para con otras entidades financieras y derivada de otras entidades financieras, y evaluarán las ciberamenazas y vulnerabilidades en materia de TIC pertinentes para sus funciones empresariales sustentadas por TIC, activos de información y activos de TIC. Las entidades financieras revisarán periódicamente, y al menos una vez al año, los escenarios de riesgo que les afecten.

3. Las entidades financieras que no sean microempresas llevarán a cabo una evaluación del riesgo cada vez que se produzca un cambio importante en la infraestructura de las redes y los sistemas de información, en los procesos o procedimientos que afecten a sus funciones empresariales sustentadas por TIC, activos de información o activos de TIC.

4. Las entidades financieras identificarán todos los activos de información y activos de TIC, incluidos los que se encuentren en emplazamientos remotos, recursos de red y equipos de *hardware*, y cartografiarán aquellos considerados esenciales. Cartografiarán la configuración de los activos de información y activos de TIC y los vínculos e interdependencias entre los distintos activos de información y activos de TIC.

5. Las entidades financieras identificarán y documentarán todos los procesos que dependan de proveedores terceros de servicios de TIC, e identificarán las interconexiones con proveedores terceros de servicios de TIC que presten servicios que sustenten funciones esenciales o importantes.

6. A los efectos de los apartados 1, 4 y 5, las entidades financieras mantendrán los inventarios pertinentes y los actualizarán periódicamente y cada vez que se produzcan los cambios importantes a que se refiere el apartado 3.

7. Las entidades financieras que no sean microempresas llevarán a cabo periódicamente, y al menos una vez al año, una evaluación específica del riesgo relacionado con las TIC en todos los sistemas de TIC heredados y, en cualquier caso, antes y después de conectar tecnologías, aplicaciones o sistemas.

Artículo 9

Protección y prevención

1. Con el fin de proteger adecuadamente los sistemas de TIC y con vistas a organizar medidas de respuesta, las entidades financieras realizarán un seguimiento y un control permanentes de la seguridad y el funcionamiento de los sistemas y herramientas de TIC y minimizarán las repercusiones en dichos sistemas del riesgo relacionado con las TIC mediante el despliegue de herramientas, políticas y procedimientos adecuados en materia de seguridad de las TIC.

2. Las entidades financieras diseñarán, adquirirán y aplicarán políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC que tengan por objeto asegurar la resiliencia, la continuidad y la disponibilidad de los sistemas de TIC, en particular aquellos que sustentan funciones esenciales o importantes, así como mantener elevados niveles de disponibilidad, autenticidad, integridad y confidencialidad de los datos, con independencia de que estén en reposo, en uso o en tránsito.

3. A fin de alcanzar los objetivos mencionados en el apartado 2, las entidades financieras utilizarán soluciones y procesos de TIC que sean adecuados de conformidad con el artículo 4. Dichas soluciones y procesos de TIC deberán:

a) garantizar la seguridad de los medios de transmisión de datos;

b) minimizar el riesgo de corrupción o pérdida de datos, acceso no autorizado y defectos técnicos que puedan obstaculizar la actividad empresarial;

c) evitar la falta de disponibilidad, el menoscabo de la autenticidad e integridad, la vulneración de la confidencialidad y la pérdida de datos;

d) garantizar que los datos estén protegidos de riesgos derivados de su gestión, incluidos los debidos a una mala administración, los relacionados con el tratamiento y los errores humanos.

4. Como parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, las entidades financieras deberán:

a) elaborar y documentar una política de seguridad de la información que defina normas para proteger la confidencialidad, disponibilidad, integridad o autenticidad de los datos, activos de información y activos de TIC, incluidos los de sus clientes, en su caso;

b) siguiendo un enfoque basado en el riesgo, establecer una estructura de gestión sólida de redes e infraestructuras utilizando técnicas, métodos y protocolos adecuados que puedan incluir la aplicación de mecanismos automatizados para aislar los activos de información afectados en caso de ciberataques;

c) aplicar políticas que limiten el acceso físico o lógico a los activos de información y activos de TIC a lo que sea necesario únicamente para funciones y actividades legítimas y aprobadas, y establecer a tal fin un conjunto de políticas, procedimientos y controles que se centren en los derechos de acceso y garanticen una buena administración de estos;

d) aplicar políticas y protocolos para mecanismos de autenticación fuerte, basados en estándares pertinentes y sistemas de control específicos, y medidas de protección de las claves criptográficas mediante las que se cifran los datos en función de los resultados de los procesos aprobados de clasificación de datos y evaluación de riesgos relacionados con las TIC;

e) aplicar políticas, procedimientos y controles documentados para la gestión de los cambios en las TIC, incluidos los cambios en el *software*, el *hardware*, los componentes de *firmware*, los sistemas o los parámetros de seguridad, que se basen en un enfoque de evaluación de riesgos y formen parte integrante del proceso general de gestión de cambios de la entidad financiera, a fin de garantizar que todos los cambios en los sistemas de TIC se registren, sometan a prueba, evalúen, aprueben, apliquen y verifiquen de forma controlada;

f) contar con políticas documentadas adecuadas y globales para los parches y actualizaciones.

A efectos del párrafo primero, letra b), las entidades financieras diseñarán la infraestructura de conexión a la red de manera que permita su ruptura o segmentación instantánea con el fin de minimizar y prevenir el contagio, especialmente en los procesos financieros interconectados.

A efectos del párrafo primero, letra e), el proceso de gestión de cambios en las TIC será aprobado por los niveles directivos adecuados y dispondrá de protocolos específicos.

Artículo 10

Detección

1. Las entidades financieras dispondrán de mecanismos para detectar rápidamente las actividades anómalas, de conformidad con el artículo 17, incluidos los problemas de rendimiento de las redes de TIC y los incidentes relacionados con las TIC, y para identificar los posibles puntos únicos de fallo significativos.

Todos los mecanismos de detección mencionados en el párrafo primero se someterán a pruebas periódicas de conformidad con el artículo 25.

2. Los mecanismos de detección a que se refiere el apartado 1 permitirán múltiples niveles de control, definirán criterios y umbrales de alerta para activar e iniciar procesos de respuesta a incidentes relacionados con las TIC, incluidos mecanismos automáticos de alerta para el personal responsable de la respuesta a incidentes relacionados con las TIC.

3. Las entidades financieras dedicarán recursos y capacidades suficientes al seguimiento de la actividad de los usuarios y la aparición de anomalías en las TIC y de incidentes relacionados con las TIC, en particular de ciberataques.

4. Los proveedores de servicios de suministro de datos dispondrán además de sistemas que permitan controlar de manera efectiva la exhaustividad de los informes de operaciones, detectar omisiones y errores manifiestos y solicitar la retransmisión de tales informes.

Artículo 11

Respuesta y recuperación

1. Como parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, y sobre la base de los requisitos de identificación establecidos en el artículo 8, las entidades financieras pondrán en práctica una política global de continuidad de la actividad en materia de TIC, que podrá ser adoptada como una política específica propia que forme parte integrante de la política global de continuidad de la actividad de la entidad financiera.

2. Las entidades financieras aplicarán la política de continuidad de la actividad en materia de TIC mediante disposiciones, planes, procedimientos y mecanismos específicos, adecuados y documentados destinados a:

a) garantizar la continuidad de las funciones esenciales o importantes de la entidad financiera;

b) responder a todos los incidentes relacionados con las TIC y resolverlos rápida, adecuada y eficazmente de manera que se limiten los daños y se dé prioridad a la reanudación de las actividades y a las acciones de recuperación;

c) activar, sin demora, planes específicos que permitan recurrir a medidas de contención, procesos y tecnologías adaptados a cada tipo de incidente relacionado con las TIC y que eviten nuevos daños, así como a procedimientos de respuesta y recuperación adaptados establecidos de conformidad con el artículo 12;

d) estimar con carácter preliminar las repercusiones, daños y pérdidas;

e) definir acciones de comunicación y gestión de crisis que garanticen la transmisión de información actualizada a todo el personal interno y las partes interesadas externas pertinentes de conformidad con el artículo 14, y su notificación a las autoridades competentes de conformidad con el artículo 19.

3. Como parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, las entidades financieras aplicarán planes conexos de respuesta y recuperación en materia de TIC que, en el caso de entidades financieras que no sean microempresas, estarán sujetos a auditorías internas independientes.

4. Las entidades financieras establecerán, mantendrán y someterán a prueba periódicamente planes adecuados de continuidad de las actividades de TIC, en particular en lo que se refiere a las funciones esenciales o importantes externalizadas o contratadas mediante acuerdos con proveedores terceros de servicios de TIC.

5. Como parte de la política global de continuidad de la actividad, las entidades financieras llevarán a cabo un análisis de impacto en el negocio de sus exposiciones a perturbaciones graves de la actividad. En el marco de dicho análisis, las entidades financieras evaluarán el impacto potencial de las perturbaciones graves de la actividad mediante criterios cuantitativos y cualitativos, utilizando datos internos y externos y análisis de escenarios, según proceda. El análisis de impacto en el negocio tendrá en cuenta el carácter esencial de las funciones empresariales identificadas y cartografiadas, los procesos de apoyo, las dependencias de terceros y los activos de información, así como sus interdependencias. Las entidades financieras garantizarán que los activos de TIC y los servicios de TIC se diseñen y utilicen en plena consonancia con el análisis de impacto en el negocio, en particular en lo que se refiere a garantizar adecuadamente la redundancia de todos los componentes esenciales.

6. Como parte de su gestión global del riesgo relacionado con las TIC, las entidades financieras:

a) someterán a prueba los planes de continuidad de la actividad y los planes de respuesta y recuperación en materia de TIC en relación con los sistemas de TIC que sustenten todas las funciones al menos una vez al año, así como en caso de que se produzca cualquier cambio sustancial en los sistemas de TIC que sustenten funciones esenciales o importantes;

b) someterán a prueba los planes de comunicación en caso de crisis establecidos de conformidad con el artículo 14.

A efectos del párrafo primero, letra a), las entidades financieras que no sean microempresas incluirán, en los planes de pruebas, escenarios de ciberataques y de conmutación entre la infraestructura primaria de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes necesarias para cumplir con las obligaciones establecidas en el artículo 12.

Las entidades financieras revisarán periódicamente su política de continuidad de la actividad en materia de TIC y sus planes de respuesta y recuperación en materia de TIC teniendo en cuenta los resultados de las pruebas realizadas de conformidad con el párrafo primero y las recomendaciones derivadas de los controles de auditoría o las revisiones supervisoras.

7. Las entidades financieras que no sean microempresas dispondrán de una función de gestión de crisis que, en caso de activación de sus planes de continuidad de la actividad en materia de TIC o de sus planes de respuesta y recuperación en materia de TIC, establecerá, entre otros, procedimientos claros para gestionar las comunicaciones de crisis internas y externas de conformidad con el artículo 14.

8. Las entidades financieras mantendrán registros fácilmente accesibles de las actividades antes de las perturbaciones y durante estas cuando se activen sus planes de continuidad de la actividad en materia de TIC y sus planes de respuesta y recuperación en materia de TIC.

9. Los depositarios centrales de valores facilitarán a las autoridades competentes copias de los resultados de las pruebas de continuidad de la actividad en materia de TIC, o de ejercicios similares.

10. Las entidades financieras que no sean microempresas informarán a las autoridades competentes, si estas lo solicitan, una estimación de los costes y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC.

11. De conformidad con el artículo 16 del Reglamento (UE) n.º 1093/2010, el artículo 16 del Reglamento (UE) n.º 1094/2010 y el artículo 16 del Reglamento (UE) n.º 1095/2010, las Autoridades Europeas de Supervisión, a través del Comité Mixto, elaborarán, a más tardar el 17 de julio de 2024, directrices comunes sobre la estimación de los costes y pérdidas anuales agregados a que se refiere el apartado 10.

Artículo 12

Políticas y procedimientos de respaldo y procedimientos y métodos de restablecimiento y recuperación

1. Con el fin de garantizar el restablecimiento de los sistemas de TIC y los datos con un tiempo mínimo de inactividad y una perturbación y pérdida limitadas, como parte de su marco de gestión del riesgo relacionado con las TIC, las entidades financieras desarrollarán y documentarán:

a) políticas y procedimientos de respaldo que especifiquen el alcance de los datos objeto de respaldo y la frecuencia mínima de este, en función del carácter esencial de la información o del nivel de confidencialidad de los datos;

b) procedimientos y métodos de restablecimiento y recuperación.

2. Las entidades financieras establecerán sistemas de respaldo que puedan activarse de conformidad con las políticas y procedimientos de respaldo, así como procedimientos y métodos de restablecimiento y recuperación. La activación de sistemas de respaldo no pondrá en peligro la seguridad de las redes y los sistemas de información ni la disponibilidad, autenticidad, integridad o confidencialidad de los datos. Las pruebas de los procedimientos de respaldo y restablecimiento y los procedimientos y métodos de recuperación se llevarán a cabo periódicamente.

3. Al restablecer los datos de seguridad mediante sus propios sistemas, las entidades financieras utilizarán sistemas de TIC que estén separados, física y lógicamente, del sistema de TIC de origen. Los sistemas de TIC estarán protegidos de forma segura contra cualquier acceso no autorizado o corrupción de las TIC y permitirán el rápido restablecimiento de los servicios utilizando los respaldos de los sistemas y los datos que sean necesarios.

En el caso de las entidades de contrapartida central, los planes de recuperación permitirán la recuperación de todas las operaciones en el momento de la perturbación, para que la entidad de contrapartida central pueda seguir operando de manera segura y finalizar la liquidación en la fecha programada.

Los proveedores de servicios de suministro de datos mantendrán además recursos suficientes y dispondrán de instalaciones de respaldo y restablecimiento para ofrecer y mantener sus servicios en todo momento.

4. Las entidades financieras que no sean microempresas mantendrán capacidades de TIC redundantes provistas de recursos, medios y funciones adecuados para satisfacer las necesidades empresariales. Las microempresas evaluarán la necesidad de mantener estas capacidades de TIC redundantes sobre la base de su perfil de riesgo.

5. Los depositarios centrales de valores mantendrán al menos un centro de tratamiento secundario dotado de recursos, capacidades, funciones y personal adecuados para satisfacer las necesidades empresariales.

El centro de proceso secundario deberá:

a) estar situado a una determinada distancia geográfica del centro de proceso primario para garantizar que presente un perfil de riesgo distinto y evitar que se vea afectado por el suceso que haya afectado al centro primario;

b) ser capaz de garantizar la continuidad de las funciones esenciales o importantes del mismo modo que el centro primario, o de prestar el nivel de servicios necesario para garantizar que la entidad financiera realice sus operaciones esenciales dentro de los objetivos de recuperación;

c) estar inmediatamente accesible para el personal de la entidad financiera a fin de garantizar la continuidad de las funciones esenciales o importantes en caso de que el centro de proceso primario no esté disponible.

6. Al determinar los objetivos de tiempo y punto de recuperación para cada función, las entidades financieras tendrán en cuenta si se trata de una función esencial o importante y las posibles repercusiones globales en la eficiencia del mercado. Estos objetivos garantizarán que, en situaciones extremas, se alcancen los niveles de servicio acordados.

7. Al recuperarse de un incidente relacionado con las TIC, las entidades financieras realizarán las comprobaciones necesarias, incluidas múltiples comprobaciones y conciliaciones, a fin de garantizar que se mantenga el máximo nivel de integridad de los datos. Estas comprobaciones también se llevarán a cabo cuando se reconstruyan datos de partes interesadas externas, a fin de garantizar que todos los datos sean coherentes entre los sistemas.

Artículo 13

Aprendizaje y evolución

1. Las entidades financieras dispondrán de capacidades y de personal para recopilar información sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC, en particular ciberataques, y para analizar las repercusiones que es probable que tengan en su resiliencia operativa digital.

2. Las entidades financieras llevarán a cabo revisiones tras incidentes relacionados con las TIC después de que un incidente grave relacionado con las TIC perturbe sus actividades principales, analizando sus causas e identificando las mejoras necesarias para las operaciones de TIC o en la política de continuidad de la actividad en materia de TIC a que se refiere el artículo 11.

Las entidades financieras que no sean microempresas comunicarán, previa petición, a las autoridades competentes los cambios que se hayan introducido después de las revisiones tras incidentes relacionados con las TIC a que se refiere el párrafo primero.

Las revisiones tras incidentes relacionados con las TIC a que se refiere el párrafo primero determinarán si se han seguido los procedimientos establecidos y si las medidas adoptadas han sido eficaces, inclusive en relación con lo siguiente:

a) la rapidez a la hora de responder a las alertas de seguridad y determinar las repercusiones de los incidentes relacionados con las TIC y su gravedad;

b) la calidad y rapidez en la realización de un análisis forense, cuando se considere oportuno;

c) la eficacia de la activación de los niveles sucesivos de intervención en caso de incidente dentro de la entidad financiera;

d) la eficacia de la comunicación interna y externa.

3. Las enseñanzas derivadas de las pruebas de resiliencia operativa digital llevadas a cabo de conformidad con los artículos 26 y 27 y de los incidentes reales relacionados con las TIC, en particular los ciberataques, junto con los problemas que se hayan planteado al activar los planes de continuidad de la actividad en materia de TIC y los planes de respuesta y recuperación en materia de TIC, además de la información pertinente intercambiada con las contrapartes y evaluada durante las revisiones supervisoras, se incorporarán debidamente de forma continua al proceso de evaluación del riesgo relacionado con las TIC. Tales hallazgos conformarán la base para las revisiones adecuadas de los componentes pertinentes del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1.

4. Las entidades financieras harán un seguimiento de la efectividad de la aplicación de su estrategia de resiliencia operativa digital establecida en el artículo 6, apartado 8. Cartografiarán la evolución del riesgo relacionado con las TIC a lo largo del tiempo, analizarán la frecuencia, los tipos, la magnitud y la evolución de los incidentes relacionados con las TIC, en particular los ciberataques y sus patrones, con el fin de comprender el nivel de exposición al riesgo relacionado con las TIC, en particular por cuanto atañe a funciones esenciales o importantes, y mejorar la madurez y preparación cibernéticas de la entidad financiera.

5. El personal directivo responsable de las TIC informará al menos una vez al año al órgano de dirección de los hallazgos a que se refiere el apartado 3 y formulará recomendaciones.

6. Las entidades financieras desarrollarán programas de sensibilización en materia de seguridad de las TIC y formación sobre resiliencia operativa digital, que constituirán módulos obligatorios en sus programas de formación del personal. Esos programas y acciones formativas serán aplicables a todos los empleados y al personal de alta dirección y tendrán un nivel de complejidad acorde con las atribuciones de sus funciones. Cuando proceda, las entidades financieras también incluirán a proveedores terceros de servicios de TIC en sus planes de formación pertinentes de conformidad con el artículo 30, apartado 2, letra i).

7. Las entidades financieras que no sean microempresas supervisarán continuamente los avances tecnológicos pertinentes, también con vistas a comprender las posibles repercusiones del despliegue de esas nuevas tecnologías en los requisitos de seguridad de las TIC y la resiliencia operativa digital. Se mantendrán al día de los últimos procesos de gestión del riesgo relacionado con las TIC, para luchar efectivamente contra las formas existentes o nuevas de ciberataques.

Artículo 14

Comunicación

1. Como parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, las entidades financieras dispondrán de planes de comunicación de crisis que permitan la divulgación responsable de, al menos, los incidentes graves relacionados con las TIC o las vulnerabilidades importantes a clientes y contrapartes, así como al público, según proceda.

2. Como parte del marco de gestión del riesgo relacionado con las TIC, las entidades financieras aplicarán políticas de comunicación destinadas al personal interno y a las partes interesadas externas. Las políticas de comunicación destinadas al personal tendrán en cuenta la necesidad de diferenciar entre el personal que participa en la gestión del riesgo relacionado con las TIC, en particular el personal responsable de la respuesta y la recuperación, y el personal al que es necesario informar.

3. Al menos una persona de la entidad financiera se encargará de aplicar la estrategia de comunicación sobre incidentes relacionados con las TIC y desempeñará a tal efecto la función de portavoz ante el público y los medios de comunicación.

Artículo 15

Mayor armonización de las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC

Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en consulta con la Agencia de la Unión Europea para la Ciberseguridad (ENISA), desarrollará normas técnicas de regulación comunes a fin de:

a) especificar otros elementos que deban incluirse en las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, con vistas a garantizar la seguridad de las redes, activar salvaguardias adecuadas contra las intrusiones y el uso indebido de los datos, preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, incluidas las técnicas criptográficas, y garantizar una transmisión exacta y rápida de los datos sin perturbaciones importantes ni demoras indebidas;

b) desarrollar nuevos componentes de los controles de los derechos de gestión de accesos a que se refiere el artículo 9, apartado 4, letra c), y la correspondiente política de recursos humanos, especificando los derechos de acceso, los procedimientos de concesión y revocación de derechos, el seguimiento de comportamientos anómalos en relación con los riesgos relacionados con las TIC a través de indicadores adecuados, también para los patrones de uso de la red, las horas, la actividad informática y los dispositivos desconocidos;

c) desarrollar más detalladamente los mecanismos especificados en el artículo 10, apartado 1, que permitan la rápida detección de actividades anómalas y los criterios establecidos en el artículo 10, apartado 2, que activen los procesos de detección de incidentes relacionados con las TIC y de respuesta a los mismos;

d) especificar más detalladamente los componentes de la política de continuidad de la actividad en materia de TIC a que se refiere el artículo 11, apartado 1;

e) especificar más detalladamente las pruebas de los planes de continuidad de la actividad en materia de TIC a que se refiere el artículo 11, apartado 6, a fin de garantizar que dichas pruebas tengan debidamente en cuenta los escenarios en los que la calidad de la ejecución de una función esencial o importante se deteriore hasta un nivel inaceptable o falle, así como el impacto potencial de la insolvencia u otros fallos de cualquier proveedor tercero de servicios de TIC pertinente y, cuando proceda, los riesgos políticos en los países o territorios de los proveedores de que se trate;

f) especificar más detalladamente los componentes de los planes de respuesta y recuperación en materia de TIC a que se refiere el artículo 11, apartado 3;

g) especificar en mayor medida el contenido y el formato del informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 5.

Al desarrollar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión deberán tener en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, la escala y la complejidad de sus servicios, actividades y operaciones, y tener al mismo tiempo debidamente presente cualquier característica específica derivada de la distinta naturaleza de las actividades en los distintos sectores de los servicios financieros.

Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de enero de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Artículo 16

Marco simplificado de gestión del riesgo relacionado con las TIC

1. Los artículos 5 a 15 del presente Reglamento no se aplicarán a las empresas de servicios de inversión pequeñas y no interconectadas ni a las entidades de pago exentas en virtud de la Directiva (UE) 2015/2366; ni a las entidades exentas en virtud de la Directiva 2013/36/UE respecto de las cuales los Estados miembros hayan decidido no aplicar la opción a que se refiere el artículo 2, apartado 4, del presente Reglamento, ni a las entidades de dinero electrónico exentas en virtud de la Directiva 2009/110/CE; ni a los fondos de pensiones de empleo pequeños.

Sin perjuicio de lo dispuesto en el párrafo primero, las entidades enumeradas en el párrafo primero deberán:

a) crear y mantener un marco de gestión sólido y documentado de riesgos relacionados con las TIC en el que se detallen los mecanismos y las medidas encaminados a procurar una gestión rápida, efectiva y global del riesgo relacionado con las TIC, incluida la protección de las infraestructuras y los componentes físicos pertinentes;

b) supervisar de manera permanente la seguridad y el funcionamiento de todos los sistemas de TIC;

c) minimizar las consecuencias del riesgo relacionado con las TIC mediante el uso de sistemas, protocolos y herramientas de TIC sólidos, resilientes y actualizados que sean apropiados para sustentar el desempeño de sus actividades y la prestación de servicios y para proteger adecuadamente la disponibilidad, autenticidad, integridad y confidencialidad de los datos en las redes y sistemas de información;

d) permitir que las fuentes de riesgo relacionado con las TIC y las anomalías en las redes y sistemas de información se identifiquen y detecten de inmediato y que los incidentes relacionados con las TIC se gestionen con rapidez;

e) identificar dependencias clave de proveedores terceros de servicios de TIC;

f) garantizar la continuidad de las funciones esenciales o importantes mediante planes de continuidad de la actividad y medidas de respuesta y recuperación que incluyan, al menos, medidas de respaldo y restablecimiento de datos;

g) someter a pruebas periódicas los planes y medidas a que se refiere la letra f), así como la eficacia de los controles llevados a cabo de conformidad con las letras a) y c);

h) aplicar, según proceda, las conclusiones operativas pertinentes resultantes de las pruebas a que se refiere la letra g) y de los análisis tras incidentes al proceso de evaluación del riesgo relacionado con las TIC y desarrollar, de acuerdo con las necesidades y el perfil de riesgo de TIC, programas de sensibilización en materia de seguridad de las TIC y formación en materia de resiliencia operativa digital para el personal y la dirección.

2. El marco de gestión del riesgo relacionado con las TIC a que se refiere el apartado 1, párrafo segundo, letra a), se documentará y revisará periódicamente y cuando se produzcan incidentes graves relacionados con las TIC, de conformidad con las instrucciones de supervisión. Se mejorará continuamente sobre la base de las enseñanzas derivadas de la aplicación y el seguimiento. Se presentará a la autoridad competente cuando esta lo solicite un informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC.

3. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en consulta con la ENISA, desarrollarán proyectos de normas técnicas de regulación comunes a fin de:

a) especificar más detalladamente los elementos que deben incluirse en el marco de gestión del riesgo relacionado con las TIC a que se refiere el apartado 1, párrafo segundo, letra a);

b) especificar más detalladamente los elementos en relación con los sistemas, protocolos y herramientas para minimizar las consecuencias del riesgo relacionado con las TIC a que se refiere el apartado 1, párrafo segundo, letra c), con el fin de garantizar la seguridad de las redes, permitir el establecimiento de salvaguardias adecuadas contra las intrusiones y el uso indebido de los datos y preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos;

c) especificar más detalladamente los componentes de los planes de continuidad de la actividad en materia de TIC a que se refiere el apartado 1, párrafo segundo, letra f);

d) especificar más detalladamente las normas sobre las pruebas de los planes de continuidad de la actividad y garantizar la efectividad de los controles a que se refiere el apartado 1, párrafo segundo, letra g), y asegurar que estas pruebas tengan debidamente en cuenta escenarios en los que la calidad de la ejecución de una función esencial o importante se deteriore hasta un nivel inaceptable o falle;

e) especificar más detalladamente el contenido y el formato del informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC a que se refiere el apartado 2.

A la hora de elaborar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión tendrán en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de enero de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

CAPÍTULO III

Gestión, clasificación y notificación de incidentes relacionados con las TIC

Artículo 17

Proceso de gestión de incidentes relacionados con las TIC

1. Las entidades financieras definirán, establecerán y aplicarán un proceso de gestión de incidentes relacionados con las TIC para detectar, gestionar y notificar dichos incidentes.

2. Las entidades financieras registrarán todos los incidentes relacionados con las TIC y las ciberamenazas importantes. Las entidades financieras establecerán los procedimientos y procesos adecuados para que los incidentes relacionados con las TIC sean objeto de un seguimiento, un tratamiento y una respuesta coherentes e integrados, a fin de asegurarse de que se identifiquen, se documenten y se aborden las causas subyacentes para evitar que se produzcan.

3. El proceso de gestión de incidentes relacionados con las TIC mencionado en el apartado 1:

a) establecerá indicadores de alerta temprana;

b) establecerá procedimientos para identificar, rastrear, registrar, categorizar y clasificar los incidentes relacionados con las TIC en función de su prioridad y gravedad y en función del carácter esencial de los servicios perjudicados, conforme a los criterios establecidos en el artículo 18, apartado 1;

c) asignará funciones y responsabilidades que deban activarse para los diferentes tipos y escenarios de incidentes relacionados con las TIC;

d) expondrá planes para la comunicación con el personal, las partes interesadas externas y los medios de comunicación de conformidad con el artículo 14, para la notificación a los clientes, para los procedimientos internos de traslado a la instancia jerárquica superior, que abarquen también las reclamaciones de los clientes relacionadas con las TIC, así como para el suministro de información a las entidades financieras que actúen como contraparte, según proceda;

e) garantizará que al menos los incidentes graves relacionados con las TIC se pongan en conocimiento de los altos directivos pertinentes y que se informe de ellos al órgano de dirección, explicando sus repercusiones, las medidas adoptadas como respuesta y los controles adicionales que se prevé implantar como resultado de estos incidentes graves relacionados con las TIC;

f) establecerá procedimientos de respuesta a los incidentes relacionados con las TIC para mitigar sus repercusiones y garantizar que los servicios sean nuevamente operativos y seguros de manera oportuna.

Artículo 18

Clasificación de los incidentes relacionados con las TIC y las ciberamenazas

1. Las entidades financieras clasificarán los incidentes relacionados con las TIC y determinarán su repercusión con arreglo a los siguientes criterios:

a) número y/o pertinencia de los clientes o las contrapartes financieras afectados y, cuando proceda, la cantidad o el número de transacciones afectadas por el incidente relacionado con las TIC, y si dicho incidente ha repercutido en la reputación;

b) duración del incidente relacionado con las TIC, incluida la duración de la interrupción del servicio;

c) extensión geográfica de las zonas afectadas por el incidente relacionado con las TIC, en especial si afecta a más de dos Estados miembros;

d) pérdidas de datos que el incidente relacionado con las TIC acarree, en relación con la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos;

e) carácter esencial de los servicios afectados, incluidas las transacciones y operaciones de la entidad financiera;

f) las consecuencias económicas, en particular los costes y las pérdidas directos e indirectos, del incidente relacionado con las TIC, tanto en términos absolutos como relativos.

2. Las entidades financieras clasificarán las ciberamenazas como importantes en función del carácter esencial de los servicios en situación de riesgo, incluidas las transacciones y operaciones de la entidad financiera, el número y/o la pertinencia de los clientes o de las contrapartes financieras a las que se dirigen las amenazas y la extensión geográfica de las zonas de riesgo.

3. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en consulta con el BCE y la ENISA, elaborarán proyectos de normas técnicas de regulación comunes en las que se especificará más detalladamente lo siguiente:

a) los criterios expuestos en el apartado 1, y en concreto los umbrales de importancia relativa para determinar los incidentes graves relacionados con las TIC o, según corresponda, los incidentes operativos o de seguridad graves relacionados con los pagos que son de obligada notificación con arreglo al artículo 19, apartado 1;

b) los criterios que deberán aplicar las autoridades competentes para evaluar la relevancia de los incidentes graves relacionados con las TIC o, según corresponda, los incidentes operativos o de seguridad graves relacionados con los pagos, para las autoridades competentes pertinentes de otros Estados miembros, y los detalles de las notificaciones de incidentes graves relacionados con las TIC o, según corresponda, incidentes operativos o de seguridad graves relacionados con los pagos, que deberán compartirse con otras autoridades competentes en virtud del artículo 19, apartados 6 y 7;

c) los criterios establecidos en el apartado 2 del presente artículo, incluidos umbrales de importancia relativa elevados para determinar las ciberamenazas importantes.

4. Cuando elaboren los proyectos de normas técnicas de regulación comunes a que se refiere el apartado 3 del presente artículo, las Autoridades Europeas de Supervisión tendrán en cuenta los criterios establecidos en el artículo 4, apartado 2, así como las normas internacionales, las orientaciones y las especificaciones elaboradas y publicadas por la ENISA, incluidas, cuando proceda, las especificaciones para otros sectores económicos. A efectos de la aplicación de los criterios establecidos en el artículo 4, apartado 2, las Autoridades Europeas de Supervisión tendrán debidamente en cuenta la necesidad de que las microempresas y las pequeñas y medianas empresas movilicen recursos y capacidades suficientes para garantizar una gestión rápida de los incidentes relacionado con las TIC.

Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación comunes a más tardar el 17 de enero de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el apartado 3 de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Artículo 19

Notificación de los incidentes graves relacionados con las TIC y notificación voluntaria de las ciberamenazas importantes

1. Las entidades financieras notificarán los incidentes graves relacionados con las TIC a la autoridad competente pertinente a que se refiere el artículo 46, de conformidad con el apartado 4 del presente artículo.

Cuando una entidad financiera sea supervisada por más de una autoridad nacional competente contemplada en el artículo 46, los Estados miembros designarán a una única autoridad competente autoridad competente pertinente responsable del desempeño de las funciones y tareas establecidas en el presente artículo.

Las entidades de crédito clasificadas como significativas de conformidad con el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013 notificarán los incidentes graves relacionados con las TIC a la autoridad nacional competente pertinente designada con arreglo al artículo 4 de la Directiva 2013/36/UE, que transmitirá dicho informe de forma inmediata al BCE.

A los efectos del párrafo primero, tras recopilar y analizar toda la información pertinente, las entidades financieras elaborarán la notificación inicial y los informes a que se refiere el apartado 4 del presente artículo mediante la plantilla a que se refiere el artículo 20 y los presentarán a la autoridad competente. En caso de que un impedimento técnico haga imposible la presentación de la notificación inicial mediante la plantilla, las entidades financieras presentarán la notificación a la autoridad competente por medios alternativos.

La notificación inicial y los informes a que hace referencia el apartado 4 incluirán toda la información necesaria para que la autoridad competente pueda determinar la importancia del incidente grave relacionado con las TIC y evaluar sus posibles efectos transfronterizos.

Sin perjuicio de la notificación en virtud del párrafo primero por parte de la entidad financiera a la autoridad competente pertinente, los Estados miembros podrán determinar de manera adicional que algunas entidades financieras, o todas ellas, presenten también la notificación inicial y cada uno de los informes a que se refiere el apartado 4 del presente artículo, utilizando las plantillas mencionadas en el artículo 20, a las autoridades competentes o a los equipos de respuesta a incidentes de seguridad informática (CSIRT), designados o establecidos de conformidad con la Directiva (UE) 2022/2555.

2. Las entidades financieras podrán notificar, de manera voluntaria, ciberamenazas importantes a la autoridad competente pertinente cuando consideren que la amenaza es pertinente para el sistema financiero, los usuarios del servicio o los clientes. La autoridad competente pertinente podrá transmitir esta información a otras autoridades pertinentes mencionadas en el apartado 6.

Las entidades de crédito clasificadas como significativas de conformidad con el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013 podrán, de manera voluntaria, notificar las ciberamenazas importantes a la autoridad nacional competente pertinente designada con arreglo al artículo 4 de la Directiva 2013/36/UE, que transmitirá dicho informe de forma inmediata al BCE.

Los Estados miembros podrán determinar que las entidades financieras que notifiquen voluntariamente de conformidad con el párrafo primero puedan también transmitir dicha notificación a los CSIRT designados o establecidos de conformidad con la Directiva (UE) 2022/2555.

3. Cuando se produzca un incidente grave relacionado con las TIC y tenga consecuencias para los intereses financieros de los clientes, las entidades financieras informarán sin demora indebida de dicho incidente tan pronto como tengan conocimiento del mismo, a sus clientes y les comunicarán todas las medidas que se hayan adoptado para mitigar sus efectos adversos.

En caso de ciberamenaza importante, las entidades financieras informarán, cuando proceda, a aquellos de sus clientes que pudieran verse afectados de cualquier medida de protección adecuada que estos consideren oportuno adoptar.

4. Las entidades financieras presentarán a la autoridad competente pertinente, dentro de los plazos que se establezcan de conformidad con el artículo 20, párrafo primero, letra a), inciso ii), la siguiente información:

a) una notificación inicial;

b) un informe intermedio posterior a la notificación inicial a que se refiere la letra a), tan pronto como la situación del incidente original haya cambiado considerablemente o la gestión del incidente grave relacionado con las TIC haya cambiado en función de las últimas informaciones disponibles, seguido, cuando sea necesario, de notificaciones actualizadas cada vez que se disponga de una actualización pertinente de la situación, y siempre que lo solicite expresamente la autoridad competente;

c) un informe final, cuando haya concluido el análisis de la causa subyacente, con independencia de que ya se hayan aplicado medidas paliativas, y cuando se disponga de las cifras reales de incidencia para sustituir a las estimaciones.

5. Las entidades financieras podrán externalizar, de conformidad con el Derecho sectorial de la Unión y nacional, las obligaciones de información establecidas en el presente artículo a un proveedor tercero de servicios. En el caso de tal externalización, la entidad financiera seguirá siendo plenamente responsable del cumplimiento de los requisitos en materia de notificación de incidentes.

6. Una vez reciba la notificación inicial y de cada uno de los informes a que se refiere el apartado 4, la autoridad competente facilitará oportunamente información detallada sobre el incidente grave relacionado con las TIC a los siguientes destinatarios en función, según proceda, de sus competencias respectivas:

a) la ABE, la AEVM o la AESPJ;

b) el BCE en el caso de las entidades financieras a que se refiere el artículo 2, apartado 1, letras a), b) y d);

c) las autoridades competentes, los puntos de contacto únicos o los CSIRT designados o establecidos de conformidad con la Directiva (UE) 2022/2555;

d) las autoridades de resolución a que se refiere el artículo 3 de la Directiva 2014/59/UE, y la Junta Única de Resolución con respecto a las entidades a que se refiere el artículo 7, apartado 2, del Reglamento (UE) n.º 806/2014 del Parlamento Europeo y del Consejo ([37]) y con respecto a las entidades y grupos a que se refiere el artículo 7, apartado 4, letra b), y apartado 5, del Reglamento (UE) n.º 806/2014 en caso de que dicha información detallada haga referencia a incidentes que suponen un riesgo para garantizar funciones esenciales en el sentido del artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE, y

e) otras autoridades públicas pertinentes con arreglo al Derecho nacional.

7. Una vez recibida la información de conformidad con el apartado 6, la ABE, la AEVM o la AESPJ y el BCE, en consulta con la ENISA y en cooperación con la autoridad competente pertinente, evaluarán si el incidente grave relacionado con las TIC es pertinente para las autoridades competentes de otros Estados miembros. Tras esta evaluación, la ABE, la AEVM o la AESPJ notificarán en consecuencia lo antes posible a las autoridades competentes pertinentes de otros Estados miembros. El BCE notificará las cuestiones pertinentes para el sistema de pagos a los miembros del Sistema Europeo de Bancos Centrales. Basándose en dicha notificación, las autoridades competentes tomarán, en su caso, las medidas necesarias para proteger la estabilidad inmediata del sistema financiero.

([37]) Reglamento (UE) n.º 806/2014 del Parlamento Europeo y del Consejo, de 15 de julio de 2014, por el que se establecen normas uniformes y un procedimiento uniforme para la resolución de entidades de crédito y de determinadas empresas de servicios de inversión en el marco de un Mecanismo Único de Resolución y un Fondo Único de Resolución y se modifica el Reglamento (UE) n.º 1093/2010 (DO L 225 de 30.7.2014, p. 1).

8. La notificación que debe efectuar la AEVM en virtud del apartado 7 del presente artículo se entiende sin perjuicio de la responsabilidad de la autoridad competente de transmitir urgentemente la información detallada sobre el incidente grave relacionado con las TIC a la autoridad pertinente del Estado miembro de acogida cuando un depositario central de valores tenga una actividad transfronteriza significativa en el Estado miembro de acogida, cuando el incidente grave relacionado con las TIC pueda tener consecuencias graves para los mercados financieros del Estado miembro de acogida y cuando existan acuerdos de cooperación entre las autoridades competentes en relación con la supervisión de las entidades financieras.

Artículo 20

Armonización del contenido de la información y las plantillas para presentarla

Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en consulta con la ENISA y el BCE, elaborarán:

a) proyectos de normas técnicas de regulación comunes a fin de:

   i) establecer el contenido de los informes respecto de incidentes graves relacionados con las TIC, a fin de reflejar los criterios establecidos en el artículo 18, apartado 1, e incorporar elementos adicionales, como información detallada para determinar la pertinencia de la información para otros Estados miembros y si constituye o no un incidente operativo o de seguridad grave relacionado con los pagos,

   ii) determinar los plazos para la notificación inicial y para cada uno de los informes a que se refiere el artículo 19, apartado 4,

   iii) establecer el contenido de la notificación en el caso de las ciberamenazas importantes.

   Al elaborar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión tendrán en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones, en particular con el fin de garantizar que, a los efectos de la letra a), inciso ii), del presente párrafo, se puedan reflejar con plazos diferentes, en su caso, las particularidades de los sectores financieros, sin perjuicio del mantenimiento de un enfoque coherente de la notificación de incidentes relacionados con las TIC en virtud del presente Reglamento y de la Directiva (UE) 2022/2555. Las Autoridades Europeas de Supervisión justificarán, en su caso, las desviaciones de los enfoques adoptados en el contexto de dicha Directiva;

b) proyectos de normas técnicas de ejecución comunes para establecer los formularios, las plantillas y los procedimientos normalizados que deberán aplicar las entidades financieras para informar de un incidente grave relacionado con las TIC y para notificar una ciberamenaza importante.

Las Autoridades Europeas de Supervisión presentarán a la Comisión los proyectos de normas técnicas de regulación comunes a que se refiere el párrafo primero, letra a), y los proyectos de normas técnicas de ejecución comunes a que se refiere el párrafo primero, letra b), a más tardar el 17 de julio de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero, letra a), del presente artículo de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Se otorgan a la Comisión competencias para adoptar las normas técnicas de ejecución a que se refiere el párrafo primero, letra b), del presente artículo de conformidad con el artículo 15 del Reglamento (UE) n.º 1093/2010, el artículo 15 del Reglamento (UE) n.º 1094/2010 y el artículo 15 del Reglamento (UE) n.º 1095/2010.

Artículo 21

Centralización de la información sobre los incidentes graves relacionados con las TIC

1. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en consulta con el BCE y la ENISA, prepararán un informe conjunto en el que se evaluará la viabilidad de centralizar más la información sobre incidentes mediante la creación de un centro único de la UE para la presentación de información sobre incidentes graves relacionados con las TIC por las entidades financieras. En el informe conjunto se estudiarán maneras de facilitar la circulación de la información sobre incidentes graves relacionados con las TIC, reducir los costes asociados y sustentar análisis temáticos con el fin de mejorar la convergencia de la supervisión.

2. El informe conjunto al que se refiere el apartado 1 incluirá al menos los siguientes elementos:

a) requisitos indispensables para la creación de un centro único de la UE;

b) ventajas, limitaciones y riesgos, incluidos los riesgos asociados a la elevada concentración de información sensible;

c) la capacidad necesaria para garantizar la interoperabilidad con respecto a otros sistemas de notificación pertinentes;

d) elementos de gestión operativa;

e) condiciones de participación;

f) modalidades técnicas de acceso al centro único de la UE para las entidades financieras y las autoridades nacionales competentes;

g) evaluación preliminar de los costes financieros que conllevaría la creación de la plataforma operativa que sustentaría el centro único de la UE, incluidos los conocimientos especializados necesarios.

3. Las Autoridades Europeas de Supervisión presentarán el informe a que se refiere el apartado 1 al Parlamento Europeo, al Consejo y a la Comisión a más tardar el 17 de enero de 2025.

Artículo 22

Observaciones de las autoridades de supervisión

1. Sin perjuicio de las aportaciones técnicas, el asesoramiento o las medidas correctoras y el seguimiento posterior que puedan facilitar, cuando proceda y de conformidad con el Derecho nacional, los CSIRT con arreglo a la Directiva (UE) 2022/2555, la autoridad competente, tras recibirlos, deberá acusar recibo de la notificación inicial y de cada uno de los informes a que se refiere el artículo 19, apartado 4, podrá, cuando sea posible, proporcionar de forma oportuna a la entidad financiera observaciones pertinentes y proporcionadas u orientación de alto nivel, en particular poniendo a su disposición cualquier información o inteligencia anonimizadas pertinentes relativas a amenazas similares, y podrá abordar las medidas correctoras aplicadas a nivel de la entidad financiera y las formas de minimizar y mitigar las repercusiones negativas en el sector financiero. Sin perjuicio de las observaciones de las autoridades de supervisión, las entidades financieras seguirán siendo plenamente responsables de la gestión de los incidentes relacionados con las TIC notificados en virtud del artículo 19, apartado 1, así como de sus consecuencias.

2. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, informarán anualmente, utilizando datos anonimizados y agregados, sobre los incidentes graves relacionados con las TIC, a cuyo respecto las autoridades competentes facilitarán información detallada de conformidad con el artículo 19, apartado 6, indicando al menos el número de incidentes graves relacionados con las TIC, su naturaleza y su repercusión en las operaciones de las entidades financieras o de los clientes, las medidas correctoras tomadas y los costes soportados.

Las Autoridades Europeas de Supervisión emitirán advertencias y elaborarán estadísticas de alto nivel para apoyar las evaluaciones de las amenazas y las vulnerabilidades que afecten a las TIC.

Artículo 23

Incidentes operativos o de seguridad relacionados con los pagos que atañen a entidades de crédito, entidades de pago, proveedores de servicios de información sobre cuentas y entidades de dinero electrónico

Los requisitos establecidos en el presente capítulo se aplicarán también a los incidentes operativos o de seguridad, graves o no, relacionados con los pagos cuando atañan a entidades de crédito, entidades de pago, proveedores de servicios de información sobre cuentas y entidades de dinero electrónico.

CAPÍTULO IV

Pruebas de resiliencia operativa digital

Artículo 24

Requisitos generales para la realización de pruebas de resiliencia operativa digital

1. A fin de evaluar el estado de preparación para gestionar incidentes relacionados con las TIC, o de detectar debilidades, deficiencias y carencias en materia de resiliencia operativa digital y de aplicar sin demora medidas correctoras, las entidades financieras que no sean microempresas establecerán, mantendrán y revisarán, teniendo en cuenta los criterios establecidos en el artículo 4, apartado 2, un programa de pruebas de resiliencia operativa digital sólido y completo que forme parte del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6.

2. El programa de pruebas de resiliencia operativa digital incluirá una serie de evaluaciones, pruebas, métodos, prácticas y herramientas que se aplicarán de conformidad con los artículos 25 y 26.

3. Al llevar a cabo el programa de pruebas de resiliencia operativa digital a que se refiere el apartado 1 del presente artículo, las entidades financieras que no sean microempresas seguirán un enfoque basado en el riesgo que tengan en cuenta los criterios establecidos en el artículo 4, apartado 2, considerando debidamente el panorama cambiante del riesgo relacionado con las TIC, todo riesgo específico al que la entidad financiera de que se trate esté o pueda estar expuesta, el carácter esencial de los activos de información y de los servicios prestados, así como cualquier otro factor que la entidad financiera considere apropiado.

4. Las entidades financieras que no sean microempresas garantizarán que las pruebas sean realizadas por partes independientes, ya sean internas o externas. Cuando un probador interno se encargue de realizar las pruebas, las entidades financieras dedicarán recursos suficientes y garantizarán que se evitan los conflictos de intereses durante todas las fases de constitución y ejecución de las pruebas.

5. Las entidades financieras que no sean microempresas establecerán procedimientos y políticas para ordenar por prioridades, clasificar y corregir todos los problemas descubiertos durante la realización de las pruebas y establecerán métodos de validación internos para asegurarse de que todas las debilidades, deficiencias o carencias sean tratadas de manera exhaustiva.

6. Las entidades financieras que no sean microempresas garantizarán, al menos una vez al año, que se efectúen las pruebas apropiadas de todos los sistemas y aplicaciones de TIC que sustenten funciones esenciales o importantes.

Artículo 25

Pruebas de las herramientas y los sistemas de TIC

1. El programa de pruebas de resiliencia operativa digital a que se refiere el artículo 24 dispondrá, de conformidad con los criterios establecidos en el artículo 4, apartado 2, la ejecución de las pruebas adecuadas, como evaluaciones y exploraciones de vulnerabilidad, análisis del *software* de código abierto, evaluaciones de seguridad de la red, análisis de carencias, exámenes de la seguridad física, cuestionarios y soluciones de *software* de detección, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo y pruebas de penetración.

2. Los depositarios centrales de valores y las entidades de contrapartida central realizarán evaluaciones de vulnerabilidad antes de implantar o reimplantar aplicaciones y componentes de infraestructuras y servicios de TIC que sustenten funciones esenciales o importantes de la entidad financiera nuevos o ya existentes.

3. Las microempresas realizarán las pruebas a que se refiere el apartado 1 mediante la combinación de un enfoque basado en el riesgo con una planificación estratégica de las pruebas de TIC, teniendo debidamente en cuenta la necesidad de mantener un planteamiento equilibrado entre la dimensión de los recursos y el tiempo que se asigne a las pruebas de TIC previstas en el presente artículo, por una parte, y la urgencia, el tipo de riesgo, el carácter esencial de los activos de información y de los servicios prestados, así como cualquier otro factor pertinente, incluida la capacidad de la entidad financiera para asumir riesgos calculados, por otra.

Artículo 26

Pruebas avanzadas de las herramientas, los sistemas y los procesos de TIC basadas en pruebas de penetración basadas en amenazas

1. Las entidades financieras distintas de las contempladas en el artículo 16, apartado 1, párrafo primero, y distintas de microempresas, determinadas de conformidad con el apartado 8, párrafo tercero, del presente artículo, llevarán a cabo al menos cada tres años pruebas avanzadas consistentes en pruebas de penetración basadas en amenazas. A partir del perfil de riesgo de la entidad financiera y teniendo en cuenta las circunstancias operativas, la autoridad competente podrá, en caso necesario, solicitar a la entidad financiera que reduzca o aumente esta frecuencia.

2. Cada una de las pruebas de penetración basadas en amenazas abarcará algunas o todas las funciones esenciales o importantes de una entidad financiera y se realizarán sobre los sistemas de producción activos que sustenten esas funciones.

Las entidades financieras determinarán todos los sistemas, procesos y tecnologías de TIC pertinentes subyacentes que sustenten funciones esenciales o importantes y servicios de TIC, incluidos aquellos que sustenten los servicios y funciones esenciales o importantes externalizados o contratados a proveedores terceros de servicios de TIC.

Las entidades financieras evaluarán qué funciones esenciales o importantes es necesario incluir en las pruebas de penetración basadas en amenazas. El resultado de esta evaluación determinará el alcance exacto de las pruebas de penetración basadas en amenazas y será validado por las autoridades competentes.

3. Cuando haya proveedores terceros de servicios de TIC incluidos en el ámbito de cobertura de las pruebas de penetración basadas en amenazas, la entidad financiera tomará las medidas y salvaguardias necesarias para asegurar la participación de estos proveedores terceros de servicios de TIC en las pruebas de penetración basadas en amenazas y mantendrá en todo momento la plena responsabilidad de garantizar el cumplimiento del presente Reglamento.

4. Sin perjuicio de lo dispuesto en el apartado 2, párrafos primero y segundo, cuando quepa esperar razonablemente que la participación de un proveedor tercero de servicios de TIC en las pruebas de penetración basadas en amenazas a que se refiere el apartado 3 tenga una repercusión negativa en la calidad o la seguridad de los servicios prestados por el proveedor tercero de servicios de TIC a clientes que sean entidades excluidas del ámbito de aplicación del presente Reglamento, o en la confidencialidad de los datos relacionados con dichos servicios, la entidad financiera y el proveedor tercero de servicios de TIC podrán acordar por escrito que el proveedor tercero de servicios de TIC celebre directamente un acuerdo contractual con un probador externo, a efectos de llevar a cabo, bajo la dirección de una entidad financiera designada, una prueba de penetración basada en amenazas conjunta en la que participen varias entidades financieras (prueba conjunta) a las que el proveedor tercero de servicios de TIC preste servicios de TIC.

Dicha prueba conjunta abarcará la gama pertinente de servicios de TIC que sustenten funciones esenciales o importantes contratadas por las entidades financieras al proveedor tercero de servicios de TIC en cuestión. Se considerará que la prueba conjunta es una prueba de penetración basada en amenazas realizada por las entidades financieras que participen en ella.

El número de entidades financieras que participen en la prueba conjunta se calibrará debidamente teniendo en cuenta la complejidad y los tipos de servicios de que se trate.

5. Las entidades financieras, con la cooperación de los proveedores terceros de servicios de TIC y otras partes involucradas, incluidos los probadores pero con exclusión de las autoridades competentes, aplicarán controles efectivos de gestión del riesgo para mitigar los riesgos de cualquier posible repercusión en los datos, daño de los activos y perturbación de funciones, servicios u operaciones esenciales o importantes en la propia entidad financiera, en sus contrapartes o en el sector financiero.

6. Al finalizar la prueba, y una vez que se hayan aprobado los informes y los planes correctores, la entidad financiera y, en su caso, los probadores externos facilitarán a la autoridad, designada de conformidad con los apartados 9 o 10, un resumen de los hallazgos pertinentes, los planes correctores y la documentación que demuestre que la prueba de penetración basada en amenazas se ha realizado conforme a los requisitos.

7. Las autoridades proporcionarán a las entidades financieras un informe de validación que confirme que la prueba se efectuó de conformidad con los requisitos según constan en la documentación, con el fin de permitir el reconocimiento mutuo de las pruebas de penetración basadas en amenazas entre las autoridades competentes. La entidad financiera notificará a la autoridad competente pertinente la validación, el resumen de los hallazgos pertinentes y los planes correctores.

Sin perjuicio de dicha validación, las entidades financieras seguirán siendo plenamente responsables en todo momento de las repercusiones de las pruebas a que se refiere el apartado 4.

8. Las entidades financieras contratarán, de conformidad con el artículo 27, a probadores a efectos de la realización de pruebas de penetración basadas en amenazas. Cuando las entidades financieras recurran a probadores internos para realizar pruebas de penetración basadas en amenazas, contratarán a probadores externos cada tres pruebas.

Las entidades de crédito clasificadas como significativas de conformidad con el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013 solo recurrirán a probadores externos de conformidad con el artículo 27, apartado 1, letras a) a e), del presente Reglamento.

Las autoridades competentes determinarán qué entidades financieras deberán realizar pruebas de penetración basadas en amenazas teniendo en cuenta los criterios establecidos en el artículo 4, apartado 2, basándose en la evaluación de:

a) factores relacionados con la repercusión, en particular la medida en que los servicios prestados y las actividades realizadas por la entidad financiera repercuten en el sector financiero;

b) posibles problemas de estabilidad financiera, incluido el carácter sistémico de la entidad financiera a escala de la Unión o nacional, según proceda;

c) el perfil de riesgo relacionado con las TIC específico, el nivel de madurez de las TIC de la entidad financiera o las características tecnológicas presentes.

9. Los Estados miembros podrán designar a una única autoridad pública en el sector financiero responsable de las cuestiones relacionadas con las pruebas de penetración basadas en amenazas en el sector financiero a escala nacional y le confiarán todas las competencias y tareas a tal efecto.

10. A falta de designación de conformidad con el apartado 9 del presente artículo, y sin perjuicio de la competencia para determinar las entidades financieras que están obligadas a llevar a cabo pruebas de penetración basadas en amenazas, una autoridad competente podrá delegar el ejercicio de todas o algunas de las tareas a que se refieren el presente artículo y el artículo 27 en otra autoridad nacional del sector financiero.

11. Las Autoridades Europeas de Supervisión desarrollarán, de acuerdo con el BCE proyectos de normas técnicas de regulación comunes de conformidad con el marco TIBER-EU para especificar más detalladamente:

a) los criterios utilizados a efectos de la aplicación del apartado 8, párrafo segundo;

b) los requisitos y normas que rigen el recurso a probadores internos;

c) los requisitos en relación con:

   i) el alcance de las pruebas de penetración basadas en amenazas a que se refiere el apartado 2,

   ii) la metodología y el enfoque de realización de pruebas que deberán seguirse en cada fase específica del proceso de prueba,

   iii) las fases de resultados, conclusión y adopción de medidas correctoras del proceso de prueba;

d) el tipo de cooperación en materia de supervisión y otros tipos de cooperación pertinente necesarios para llevar a cabo pruebas de penetración basadas en amenazas, así como la facilitación del reconocimiento mutuo de dichas pruebas, en el contexto de entidades financieras que operen en más de un Estado miembro, para permitir un nivel adecuado de participación de los supervisores y una ejecución flexible que tenga en cuenta las características específicas de subsectores financieros o mercados financieros locales.

Al elaborar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión tendrán debidamente en cuenta cualquier característica específica derivada de la distinta naturaleza de las actividades en los distintos sectores de los servicios financieros.

Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de julio de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Artículo 27

Requisitos aplicables a los probadores para la realización de pruebas de penetración basadas en amenazas

1. Para la realización de pruebas de penetración basadas en amenazas, las entidades financieras solo recurrirán a probadores que:

a) tengan el más alto grado de idoneidad y prestigio;

b) posean capacidades técnicas y organizativas y demuestren conocimientos especializados en inteligencia sobre amenazas, pruebas de penetración y pruebas de equipo rojo;

c) estén acreditados por un órgano de certificación de un Estado miembro o se adhieran a códigos de conducta o marcos éticos oficiales;

d) proporcionen una garantía independiente o un informe de auditoría que acrediten la buena gestión de los riesgos asociados con la realización de pruebas de penetración basadas en amenazas, incluidas la protección debida de la información confidencial de la entidad financiera y medidas de reparación en caso de riesgos empresariales para ella;

e) estén debida y completamente cubiertos por los seguros pertinentes de responsabilidad civil profesional, también frente a los riesgos de falta intencionada y negligencia.

2. En caso de recurrir a probadores internos, las entidades financieras garantizarán que se cumplan, además de todos los requisitos establecidos en el apartado 1, todas las condiciones siguientes:

a) el recurso a los probadores ha sido autorizado por la autoridad competente correspondiente o por la autoridad pública única designada de conformidad con el artículo 26, apartados 9 y 10;

b) la autoridad competente correspondiente ha verificado que la entidad financiera dispone de recursos específicos suficientes y ha garantizado que se eviten los conflictos de intereses durante todas las fases de constitución y ejecución de las pruebas, y

c) el proveedor de inteligencia sobre amenazas es externo con respecto a la entidad financiera.

3. Las entidades financieras se asegurarán de que los contratos con probadores externos exijan una buena gestión de los resultados de las pruebas de penetración basadas en amenazas y de que ningún tratamiento de datos del que sean objeto, incluido cualquier proceso de generación, almacenamiento, agregación, redacción, notificación, comunicación o destrucción cree riesgos para la entidad financiera.

CAPÍTULO V

Gestión del riesgo relacionado con las TIC derivado de terceros

Sección I

Principios fundamentales de una buena gestión del riesgo relacionado con las TIC derivado de terceros

Artículo 28

Principios generales

1. Las entidades financieras gestionarán el riesgo relacionado con las TIC derivado de terceros como un elemento integrante del riesgo relacionado con las TIC dentro de su marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 1, y de conformidad con los principios siguientes:

a) las entidades financieras que tengan acuerdos contractuales en vigor para utilizar servicios de TIC en el funcionamiento de sus operaciones comerciales serán, en todo momento, plenamente responsables del cumplimiento y observancia de todas las obligaciones con arreglo al presente Reglamento y al Derecho aplicable en materia de servicios financieros;

b) las entidades financieras gestionarán el riesgo relacionado con las TIC derivado de terceros con arreglo al principio de proporcionalidad, teniendo en cuenta:

i) la naturaleza, la escala, la complejidad y la importancia de las dependencias con respecto a las TIC,

ii) los riesgos derivados de los acuerdos contractuales sobre el uso de servicios de TIC celebrados con proveedores terceros de servicios de TIC, teniendo en cuenta el carácter esencial o la importancia del servicio, el proceso o la función de que se trate, y la repercusión potencial en la continuidad y la disponibilidad de las actividades y los servicios financieros, a escala particular y de grupo.

2. Como parte de su marco de gestión del riesgo relacionado con las TIC, las entidades financieras distintas de las entidades contempladas en el artículo 16, apartado 1, párrafo primero, y distintas de microempresas adoptarán una estrategia, que revisarán periódicamente, sobre el riesgo relacionado con las TIC derivado de terceros, teniendo en cuenta la estrategia de múltiples proveedores a que se refiere el artículo 6, apartado 9, cuando proceda. Esa estrategia relativa al riesgo relacionado con las TIC derivado de terceros incluirá una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC y se aplicará a título particular y, cuando proceda, de forma subconsolidada y consolidada. El órgano de dirección, a partir de una evaluación del perfil de riesgo general de la entidad financiera y la escala y la complejidad de los servicios empresariales, revisará periódicamente los riesgos detectados por lo que respecta a los acuerdos contractuales relativos al uso de servicios de TIC que sustenten funciones esenciales o importantes.

3. Como parte de su marco de gestión del riesgo relacionado con las TIC, las entidades financieras mantendrán y actualizarán a nivel de la entidad, y a nivel subconsolidado y consolidado, un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC.

Los acuerdos contractuales a que se refiere el párrafo primero se documentarán adecuadamente, distinguiendo entre los que comprendan servicios de TIC que sustentan funciones esenciales o importantes y los que no.

Las entidades financieras comunicarán al menos una vez al año a las autoridades competentes información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.

Las entidades financieras pondrán a disposición de la autoridad competente que lo solicite el registro completo de información o, cuando así se solicite, secciones específicas de este, junto con toda información que se considere necesaria para permitir la supervisión efectiva de la entidad financiera.

Las entidades financieras informarán oportunamente a la autoridad competente cuando se propongan celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.

4. Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, las entidades financieras:

a) evaluarán si el acuerdo contractual se refiere al uso de servicios de TIC que sustenten una función esencial o importante;

b) evaluarán si se cumplen las condiciones de supervisión para la contratación;

c) determinarán y evaluarán todos los riesgos pertinentes en relación con el acuerdo contractual, incluida la posibilidad de que dicho acuerdo pueda contribuir a reforzar el riesgo de concentración de TIC a que se refiere el artículo 29;

d) llevarán a cabo todas las comprobaciones debidas con respecto a los posibles proveedores terceros de servicios de TIC y se asegurarán, a través de los procesos de selección y evaluación, de la idoneidad de dichos proveedores;

e) determinarán y evaluarán los conflictos de intereses que el acuerdo contractual pueda causar.

5. Las entidades financieras únicamente podrán celebrar acuerdos contractuales con proveedores terceros de servicios de TIC que cumplan estándares adecuados en materia de seguridad de la información. Cuando tales acuerdos contractuales se refieran a funciones esenciales o importantes, las entidades financieras, antes de celebrarlos, prestarán la debida consideración a la aplicación, por parte de proveedores terceros de servicios de TIC, de los estándares en materia de seguridad de la información más actualizados y más estrictos en términos de calidad.

6. Al ejercer los derechos de acceso, inspección y auditoría sobre el proveedor tercero de servicios de TIC, las entidades financieras determinarán previamente, con arreglo a un enfoque basado en el riesgo, la frecuencia de las auditorías e inspecciones y los ámbitos que deben auditarse, según normas de auditoría comúnmente aceptadas en consonancia con las instrucciones de supervisión sobre el uso y la incorporación de dichas normas de auditoría.

Cuando los acuerdos contractuales relativos al uso de servicios de TIC celebrados con proveedores terceros de servicios de TIC impliquen una gran complejidad técnica, la entidad financiera verificará que los auditores, ya sean internos, externos o un grupo de auditores, posean las capacidades y los conocimientos adecuados para llevar a cabo efectivamente las auditorías y evaluaciones pertinentes.

7. Las entidades financieras garantizarán la posibilidad de terminar los acuerdos contractuales sobre el uso de servicios de TIC en cualquiera de los siguientes casos:

a) incumplimiento importante por parte del proveedor tercero de servicios de TIC de las disposiciones legales o reglamentarias o las cláusulas contractuales aplicables;

b) circunstancias observadas durante el seguimiento del riesgo relacionado con las TIC derivado de terceros que se considere que pueden alterar el desempeño de las funciones prestadas en virtud del acuerdo contractual, incluidos cambios importantes que afecten al acuerdo o a la situación del proveedor tercero de servicios de TIC;

c) debilidades manifiestas del proveedor tercero de servicios de TIC en cuanto a su gestión global del riesgo relacionado con las TIC y, en particular, a la forma en que garantiza la disponibilidad, la autenticidad, la integridad y la confidencialidad de los datos, ya sean personales o sensibles en cualquier otro sentido, o no personales;

d) cuando la autoridad competente haya dejado de poder supervisar efectivamente a la entidad financiera como resultado de las condiciones del acuerdo contractual de que se trate o las circunstancias relacionadas con él.

8. En el caso de los servicios de TIC que sustenten funciones esenciales o importantes, las entidades financieras establecerán estrategias de salida. Las estrategias de salida tendrán en cuenta los riesgos que puedan surgir en relación con los proveedores terceros de servicios de TIC, en particular un posible fallo por su parte, un deterioro de la calidad de los servicios de TIC prestados, cualquier perturbación de la actividad debida a una falta de prestación de servicios de TIC o a una prestación inadecuada, o cualquier riesgo sustancial que pueda plantearse en relación con el ejercicio adecuado y continuo del servicio de TIC correspondiente, o la terminación de los acuerdos contractuales con proveedores terceros de servicios de TIC en cualquiera de las circunstancias enumeradas en el apartado 7.

Las entidades financieras se asegurarán de poder abandonar los acuerdos contractuales sin:

a) perturbación de sus operaciones comerciales;

b) limitación del cumplimiento de los requisitos reglamentarios;

c) perjuicio para la continuidad y la calidad de los servicios prestados a los clientes.

Los planes de salida serán globales, estarán documentados y, de conformidad con los criterios establecidos en el artículo 4, apartado 2, se someterán a suficientes pruebas y se revisarán periódicamente.

Las entidades financieras hallarán soluciones alternativas y elaborarán planes de transición que les permitan recuperar los servicios de TIC contratados y los datos pertinentes del proveedor tercero de servicios de TIC y transferirlos de forma segura e íntegra a proveedores alternativos o reincorporarlos internamente.

Las entidades financieras dispondrán de medidas de contingencia adecuadas para mantener la continuidad de la actividad en caso de que se den las circunstancias mencionadas en el párrafo primero.

9. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, elaborarán proyectos de normas técnicas de ejecución a fin de establecer las plantillas normalizadas para el registro de información a que se refiere el apartado 3, incluyendo la información común a todos los acuerdos contractuales relativa al uso de servicios de TIC. Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de ejecución a más tardar el 17 de enero de 2024.

Se otorgan a la Comisión competencias para adoptar las normas técnicas de ejecución a que se refiere el párrafo primero de conformidad con el artículo 15 del Reglamento (UE) n.º 1093/2010, el artículo 15 del Reglamento (UE) n.º 1094/2010 y el artículo 15 del Reglamento (UE) n.º 1095/2010.

10. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación a fin de especificar en más profundidad el contenido detallado de la política a que se refiere el apartado 2 en relación con los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC.

A la hora de elaborar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión tendrán en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones. Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de enero de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Artículo 29

Evaluación preliminar del riesgo de concentración de TIC a nivel de la entidad

1. Al llevar a cabo la determinación y evaluación de los riesgos a que se refiere el artículo 28, apartado 4, letra c), las entidades financieras también tendrán en cuenta si la celebración prevista de un acuerdo contractual en relación con los servicios de TIC que sustenten funciones esenciales o importantes podría dar lugar a alguna de las siguientes circunstancias:

a) la celebración de un contrato con un proveedor tercero de servicios de TIC que no sea fácilmente sustituible, o

b) la coexistencia de múltiples acuerdos contractuales en relación con la prestación de servicios de TIC que sustenten funciones esenciales o importantes con el mismo proveedor tercero de servicios de TIC o con proveedores terceros de servicios de TIC estrechamente relacionados.

Las entidades financieras ponderarán los beneficios y los costes de soluciones alternativas, como el recurso a distintos proveedores terceros de servicios de TIC, considerando si las soluciones contempladas se ajustan a las necesidades y objetivos empresariales establecidos en su estrategia de resiliencia digital y de qué manera.

2. Cuando el acuerdo contractual sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes incluya la posibilidad de que un proveedor tercero de servicios de TIC subcontrate a su vez servicios de TIC que sustenten una función esencial o importante a otros proveedores terceros de servicios de TIC, las entidades financieras ponderarán los beneficios y los riesgos que puedan derivarse de esa posible subcontratación, en particular cuando se trate de un subcontratista de TIC establecido en un tercer país.

Cuando el acuerdo contractual afecte a servicios de TIC que sustenten funciones esenciales o importantes, las entidades financieras ponderarán debidamente las disposiciones legislativas en materia de insolvencia que se aplicarían en caso de quiebra del proveedor tercero de servicios de TIC, así como cualquier restricción que pueda surgir y que afecte a la recuperación urgente de los datos de la entidad financiera.

Cuando se celebren acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes con un proveedor tercero de servicios de TIC establecido en un tercer país, las entidades financieras tendrán en consideración, además de lo mencionado el párrafo segundo, el cumplimiento de la normativa en materia de protección de datos de la Unión y la aplicación efectiva del Derecho en ese tercer país.

Cuando el acuerdo contractual sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes contemple la subcontratación, las entidades financieras evaluarán si las cadenas de subcontratación potencialmente largas o complejas pueden afectar a su capacidad para efectuar un seguimiento completo de las funciones contratadas y a la capacidad de la autoridad competente para supervisar efectivamente a la entidad financiera a este respecto, y de qué manera.

Artículo 30

Cláusulas contractuales fundamentales

1. Los derechos y obligaciones de la entidad financiera y del proveedor tercero de servicios de TIC estarán claramente asignados y establecidos por escrito. El contrato completo incluirá los acuerdos de nivel de servicio y se formalizará en un documento escrito que estará a disposición de las partes en papel, o en un documento en otro formato descargable, duradero y accesible.

2. Los acuerdos contractuales sobre el uso de servicios de TIC incluirán, como mínimo, los elementos siguientes:

a) una descripción clara y completa de todas las funciones y los servicios de TIC que deba prestar el proveedor tercero de servicios de TIC en la que se indique si está permitida la subcontratación de un servicio de TIC que sustente una función esencial o importante, o partes sustanciales de ellas, y, en caso afirmativo, las condiciones aplicables a dicha subcontratación;

b) los lugares, en concreto, las regiones o países, en los que deberán proporcionarse las funciones y los servicios de TIC contratados o subcontratados y en los que deberán tratarse los datos, incluido el lugar de almacenamiento, y el requisito de que el proveedor tercero de servicios de TIC notifique por adelantado a la entidad financiera cualquier cambio previsto de dichos lugares;

c) disposiciones sobre disponibilidad, autenticidad, integridad y confidencialidad en relación con la protección de los datos, incluidos los datos personales;

d) disposiciones sobre las garantías de la entidad financiera de poder acceder a los datos personales y no personales tratados y de poder recuperarlos y que le sean devueltos en un formato fácilmente accesible en caso de insolvencia, resolución o interrupción de las operaciones comerciales del proveedor tercero de servicios de TIC o en caso de terminación de los acuerdos contractuales;

e) descripciones del nivel de servicio, incluidas sus actualizaciones y revisiones;

f) la obligación del proveedor tercero de servicios de TIC de prestar asistencia a la entidad financiera sin coste adicional, o a un coste determinado con anterioridad, cuando se produzca un incidente de TIC relacionado con el servicio de TIC prestado a la entidad financiera;

g) la obligación del proveedor tercero de servicios de TIC de cooperar plenamente con las autoridades competentes y las autoridades de resolución de la entidad financiera, incluidas las personas nombradas por ellas;

h) los derechos de terminación y los correspondientes plazos mínimos de notificación para la terminación de los acuerdos contractuales, conforme a las expectativas de las autoridades competentes y las autoridades de resolución;

i) las condiciones para la participación de proveedores terceros de servicios de TIC en los programas de sensibilización en materia de seguridad de las TIC y en las actividades de formación sobre resiliencia operativa digital de las entidades financieras, de conformidad con el artículo 13, apartado 6.

3. Además de los elementos a que se refiere el apartado 2, los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes incluirán por lo menos lo siguiente:

a) descripciones completas del nivel de servicio, incluidas sus actualizaciones y revisiones, con objetivos precisos de rendimiento cuantitativos y cualitativos dentro de los niveles de servicio acordados, de modo que la entidad financiera pueda realizar un seguimiento efectivo de los servicios de TIC y que se puedan adoptar sin demora indebida las medidas correctoras adecuadas cuando no se alcancen los niveles de servicio acordados;

b) plazos de notificación y obligaciones de información del proveedor tercero de servicios de TIC a la entidad financiera, incluida la notificación de cualquier hecho que pueda afectar considerablemente a la capacidad del proveedor tercero de servicios de TIC para prestar de forma efectiva los servicios de TIC que sustentan funciones esenciales o importantes de conformidad con los niveles de servicio acordados;

c) requisitos para que el proveedor tercero de servicios de TIC aplique y someta apruebe los planes de contingencia empresarial y disponga de medidas, herramientas y políticas de seguridad de las TIC que proporcionen un nivel adecuado de seguridad para la prestación de servicios por parte de la entidad financiera en consonancia con su marco regulador;

d) la obligación de que el proveedor tercero de servicios de TIC participe y coopere plenamente en las pruebas de penetración basadas en amenazas de la entidad financiera a que se refieren los artículos 26 y 27;

e) el derecho a realizar un seguimiento continuo de la actuación del proveedor tercero de servicios de TIC, lo que implica lo siguiente:

i) derechos ilimitados de acceso, inspección y auditoría por la entidad financiera o un tercero designado, y por la autoridad competente, y el derecho a hacer copias de la documentación pertinente *in situ* si son esenciales para las operaciones del proveedor tercero de servicios de TIC, cuyo ejercicio efectivo no se vea obstaculizado o limitado por otros acuerdos contractuales o políticas de aplicación,

ii) el derecho a pactar niveles de garantía alternativos si se ven afectados los derechos de otros clientes,

iii) la obligación de que el proveedor tercero de servicios de TIC coopere plenamente durante las inspecciones y las auditorías *in situ* realizadas por las autoridades competentes, el supervisor principal, la entidad financiera o un tercero designado, y

iv) la obligación de proporcionar detalles sobre el alcance, los procedimientos que deben seguirse y la frecuencia de tales inspecciones y auditorías;

f) estrategias de salida, en particular el establecimiento de un período transitorio suficiente obligatorio:

i) durante el cual el proveedor tercero de servicios de TIC seguirá proporcionando las funciones o los servicios de TIC de que se trate con el fin de reducir el riesgo de perturbación en la entidad financiera o de garantizar su resolución y reestructuración efectivas,

ii) que permita a la entidad financiera migrar a otro proveedor tercero de servicios de TIC o adoptar soluciones internas coherentes con la complejidad del servicio prestado.

Como excepción a lo dispuesto en la letra e), el proveedor tercero de servicios de TIC y la entidad financiera que sea una microempresa podrán acordar que se puedan delegar los derechos de acceso, inspección y auditoría de la entidad financiera en un tercero independiente, designado por el proveedor tercero de servicios de TIC, y que la entidad financiera pueda solicitar al tercero en cualquier momento información y garantías sobre la actuación del proveedor tercero de servicios de TIC.

4. Al negociar acuerdos contractuales, las entidades financieras y los proveedores terceros de servicios de TIC considerarán el uso de cláusulas contractuales tipo elaboradas por las autoridades públicas para servicios específicos.

5. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación para especificar más detalladamente los elementos a que se refiere el apartado 2, letra a), que una entidad financiera debe determinar y evaluar a la hora de subcontratar servicios de TIC que sustenten funciones esenciales o importantes.

A la hora de elaborar dichos proyectos de normas técnicas de regulación, las Autoridades Europeas de Supervisión tendrán en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de julio de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Sección II

Marco de supervisión de los proveedores terceros esenciales de servicios de TIC

Artículo 31

Designación de proveedores terceros esenciales de servicios de TIC

1. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y por recomendación del Foro de Supervisión establecido en virtud del artículo 32, apartado 1, deberán:

a) designar a los proveedores terceros de servicios de TIC que sean esenciales para las entidades financieras, tras una evaluación que tenga en cuenta los criterios especificados en el apartado 2;

b) nombrar como supervisor principal para cada proveedor tercero esencial de servicios de TIC a la Autoridad Europea de Supervisión que sea responsable, de conformidad con los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 o (UE) n.º 1095/2010, para las entidades financieras que tengan conjuntamente la parte más grande de activos totales del valor de activos totales de todas las entidades financieras que utilizan los servicios del proveedor tercero esencial de servicios de TIC pertinente, según conste en la suma de los balances particulares de dichas entidades financieras.

2. La designación a que se refiere el apartado 1, letra a), se basará en todos los criterios siguientes en relación con los servicios de TIC prestados por el proveedor tercero de servicios de TIC:

a) el impacto sistémico en la estabilidad, la continuidad o la calidad de la prestación de servicios financieros en caso de un posible fallo operativo a gran escala del proveedor tercero de servicios de TIC de que se trate que afecte a la prestación de sus servicios, teniendo en cuenta el número de entidades financieras y el valor total de los activos de las entidades financieras a las que presta servicios el proveedor tercero de servicios de TIC de que se trate;

b) el carácter o la importancia sistémicos de las entidades financieras que dependen del proveedor tercero de servicios de TIC de que se trate, evaluados con arreglo a los parámetros siguientes:

   i) el número de entidades de importancia sistémica mundial (EISM) u otras entidades de importancia sistémica (OEIS) que dependen del proveedor tercero de servicios de TIC correspondiente,

   ii) la interdependencia entre las EISM u OEIS a que se refiere el inciso i) y otras entidades financieras, incluidas las situaciones en las que las EISM u OEIS prestan servicios de infraestructura financiera a otras entidades financieras;

c) la dependencia de las entidades financieras respecto de los servicios prestados por el proveedor tercero de servicios de TIC pertinente en relación con funciones esenciales o importantes de entidades financieras que, en última instancia, impliquen al mismo proveedor tercero de servicios de TIC, con independencia de que las entidades financieras recurran a dichos servicios directa o indirectamente, a través de acuerdos de subcontratación;

d) el grado de sustituibilidad del proveedor tercero de servicios de TIC, teniendo en cuenta los parámetros siguientes:

   i) la falta de alternativas reales, siquiera parciales, debido al número limitado de proveedores terceros de servicios de TIC activos en un mercado específico, o a la cuota de mercado del proveedor tercero de servicios de TIC de que se trate, o a la complejidad o dificultad técnica existente, entre otras cosas en relación con tecnologías protegidas por derechos, o a las características específicas de la organización o la actividad del proveedor tercero de servicios de TIC,

   ii) las dificultades relacionadas con la migración parcial o total de los datos y cargas de trabajo pertinentes del proveedor tercero de servicios de TIC en cuestión a otro, al ser considerables los costes financieros, el tiempo u otros recursos que el proceso de migración podría implicar, o debido al aumento del riesgo de TIC o de otros riesgos operativos a los que podría verse expuesta la entidad financiera a través de dicha migración.

3. Cuando el proveedor tercero de servicios de TIC pertenezca a un grupo, los criterios a que se refiere el apartado 2 se tendrán en cuenta en relación con los servicios de TIC prestados por el grupo en su conjunto.

4. Los proveedores terceros esenciales de servicios de TIC que formen parte de un grupo designarán a una persona jurídica como punto de coordinación para garantizar una representación y una comunicación adecuadas con el supervisor principal.

5. El supervisor principal notificará al proveedor tercero de servicios de TIC el resultado de la evaluación previa a la designación a que se refiere el apartado 1, letra a). En el plazo de seis semanas a partir de la fecha de la notificación, el proveedor tercero de servicios de TIC podrá presentar al supervisor principal una declaración motivada con cualquier información pertinente a efectos de la evaluación. El supervisor principal considerará la declaración motivada y podrá solicitar que se presente información adicional en un plazo de treinta días naturales a partir de la recepción de dicha declaración.

Tras designar a un proveedor tercero de servicios de TIC como esencial, las Autoridades Europeas de Supervisión, a través del Comité Mixto, notificarán al proveedor tercero de servicios de TIC dicha designación y la fecha de inicio a partir de la cual será efectivamente objeto de actividades de supervisión. Dicha fecha de inicio no será posterior en más de un mes a la notificación. El proveedor tercero de servicios de TIC notificará a las entidades financieras a las que presta servicios su designación como esencial.

6. Se otorgan a la Comisión los poderes para adoptar un acto delegado, de conformidad con el artículo 57, para completar el presente Reglamento especificando con más detalle los criterios mencionados en el apartado 2 del presente artículo, a más tardar el 17 de julio de 2024.

7. La designación a que se refiere el apartado 1, letra a), no se utilizará hasta que la Comisión haya adoptado un acto delegado de conformidad con el apartado 6.

8. La designación a que se refiere el apartado 1, letra a), no se aplicará a:

i) las entidades financieras que presten servicios de TIC a otras entidades financieras,

ii) los proveedores terceros de servicios de TIC que estén sujetos a marcos de supervisión establecidos en apoyo de las tareas a que se refiere el artículo 127, apartado 2, del TFUE,

iii) los proveedores intragrupo de servicios de TIC,

iv) los proveedores terceros de servicios de TIC que presten servicios de TIC únicamente en un Estado miembro a entidades financieras que operan exclusivamente en ese Estado miembro.

9. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, establecerán, publicarán y actualizarán anualmente la lista de proveedores terceros esenciales de servicios de TIC a escala de la Unión.

10. A efectos de lo dispuesto en el apartado 1, letra a), las autoridades competentes transmitirán anualmente y de forma agregada los informes a que se refiere el artículo 28, apartado 3, párrafo tercero, al Foro de Supervisión establecido en virtud del artículo 32. El Foro de Supervisión evaluará las dependencias de terceros en el ámbito de las TIC de las entidades financieras basándose en la información recibida de las autoridades competentes.

11. Los proveedores terceros de servicios de TIC que no estén incluidos en la lista a que se refiere el apartado 9 podrán solicitar ser designados como esenciales de conformidad con el apartado 1, letra a).

A efectos de lo dispuesto en el párrafo primero, el proveedor tercero de servicios de TIC presentará una solicitud motivada a la ABE, la AEVM o la AESPJ que, a través del Comité Mixto, decidirán si lo designan o no como esencial de conformidad con el apartado 1, letra a).

La decisión a que se refiere el párrafo segundo se adoptará y notificará al proveedor tercero de servicios de TIC en un plazo de seis meses a partir de la recepción de la solicitud.

12. Las entidades financieras solo recurrirán a los servicios de un proveedor tercero de servicios de TIC establecido en un tercer país y que haya sido designado como esencial de conformidad con el apartado 1, letra a), si este último ha establecido una filial en la Unión en los 12 meses siguientes a la designación.

13. El proveedor tercero esencial de servicios de TIC a que se refiere el apartado 12 notificará al supervisor principal cualquier cambio en la estructura de la dirección de la filial establecida en la Unión.

Artículo 32

Estructura del marco de supervisión

1. El Comité Mixto, de conformidad con el artículo 57, apartado 1, del Reglamento (UE) n.º 1093/2010, el artículo 57, apartado 1, del Reglamento (UE) n.º 1094/2010 y el artículo 57, apartado 1, del Reglamento (UE) n.º 1095/2010, establecerá el Foro de Supervisión como subcomité encargado de apoyar el trabajo del Comité Mixto y del supervisor principal a que se refiere el artículo 31, apartado 1, letra b), en materia de riesgo relacionado con las TIC derivado de terceros en los distintos sectores financieros. El Foro de Supervisión elaborará los proyectos de posiciones conjuntas y de actos comunes del Comité Mixto en este ámbito.

El Foro de Supervisión debatirá periódicamente las novedades pertinentes en materia de riesgos y vulnerabilidades en materia de TIC y promoverá un enfoque coherente de seguimiento de los riesgos relacionados con las TIC derivados de terceros a escala de la Unión.

2. El Foro de Supervisión llevará a cabo anualmente una evaluación colectiva de los resultados y las conclusiones de las actividades de supervisión realizadas para todos los proveedores terceros esenciales de servicios de TIC y promoverá medidas de coordinación para incrementar la resiliencia operativa digital de las entidades financieras, fomentar buenas prácticas para hacer frente al riesgo de concentración de TIC y estudiar medidas de mitigación de la transferencia de riesgos entre sectores.

3. El Foro de Supervisión presentará índices de referencia exhaustivos para los proveedores terceros esenciales de servicios de TIC, que el Comité Mixto adoptará como posiciones conjuntas de las Autoridades Europeas de Supervisión de conformidad con el artículo 56, apartado 1, del Reglamento (UE) n.º 1093/2010, el artículo 56, apartado 1, del Reglamento (UE) n.º 1094/2010 y el artículo 56, apartado 1, del Reglamento (UE) n.º 1095/2010.

4. El Foro de Supervisión estará integrado por:

a) los presidentes de las Autoridades Europeas de Supervisión;

b) un representante de alto nivel del personal en plantilla de la autoridad competente pertinente a que se refiere el artículo 46 de cada Estado miembro;

c) los respectivos directores ejecutivos de cada Autoridad Europea de Supervisión y un representante de la Comisión, de la JERS, del BCE y de la ENISA en calidad de observadores;

d) en su caso, un representante adicional de una autoridad competente a que se refiere el artículo 46 de cada Estado miembro, en calidad de observador;

e) cuando proceda, un representante de las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555 responsable, en calidad de observador, de la supervisión de una entidad esencial o importante sujeta a dicha Directiva, que haya sido designada proveedor tercero esencial de servicios de TIC.

Cuando proceda, el Foro de Supervisión podrá solicitar el asesoramiento de expertos independientes nombrados de conformidad con el apartado 6.

5. Cada Estado miembro designará a la autoridad competente pertinente a cuyo personal pertenecerá el representante de alto nivel a que se refiere el apartado 4, párrafo primero, letra b), e informará de ello al supervisor principal.

Las Autoridades Europeas de Supervisión publicarán en su sitio web la lista de representantes de alto nivel del personal en plantilla de la autoridad competente pertinente, designados por los Estados miembros.

6. Los expertos independientes a que se refiere el apartado 4, párrafo segundo, serán nombrados por el Foro de Supervisión, que los elegirá de entre un grupo de expertos seleccionados tras un proceso de presentación de candidaturas público y transparente.

Los expertos independientes serán nombrados en atención a sus conocimientos especializados en materia de estabilidad financiera, resiliencia operativa digital y seguridad de las TIC. Actuarán con independencia y objetividad en interés exclusivo del conjunto de la Unión y no pedirán ni aceptarán instrucción alguna de las instituciones u órganos de la Unión, de ningún Gobierno de un Estado miembro ni de ninguna otra entidad pública o privada.

7. De conformidad con el artículo 16 del Reglamento (UE) n.º 1093/2010, el artículo 16 del Reglamento (UE) n.º 1094/2010 y el artículo 16 del Reglamento (UE) n.º 1095/2010, las Autoridades Europeas de Supervisión emitirán, a más tardar el 17 de julio de 2024, a efectos de lo dispuesto en la presente sección, directrices sobre la cooperación entre ellas y las autoridades competentes que incluyan procedimientos y condiciones detallados de distribución y ejecución de tareas entre las autoridades competentes y las Autoridades Europeas de Supervisión, así como los pormenores sobre los intercambios de información necesarios para que las autoridades competentes garanticen el seguimiento de las recomendaciones formuladas en virtud del artículo 35, apartado 1, letra d), dirigidas a los proveedores terceros esenciales de servicios de TIC.

8. Los requisitos establecidos en la presente sección se entenderán sin perjuicio de la aplicación de la Directiva (UE) 2022/2555 y de otras normas de la Unión sobre supervisión aplicables a los proveedores de servicios de computación en nube.

9. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y basándose en los trabajos preparatorios realizados por el Foro de Supervisión, presentarán anualmente al Parlamento Europeo, al Consejo y a la Comisión un informe sobre la aplicación de la presente sección.

Artículo 33

Tareas del supervisor principal

1. El supervisor principal, nombrado de conformidad con el artículo 31, apartado 1, letra b), llevará a cabo la supervisión de los proveedores terceros esenciales de servicios de TIC asignados y será, a efectos de todos los asuntos relacionados con la supervisión, el punto de contacto principal para dichos proveedores terceros esenciales de servicios de TIC.

2. A efectos de lo dispuesto en el apartado 1, el supervisor principal evaluará si cada proveedor tercero esencial de servicios de TIC ha establecido normas, procedimientos, mecanismos y disposiciones completos, sólidos y efectivos para gestionar el riesgo relacionado con las TIC que pueda plantear a las entidades financieras.

La evaluación a que se refiere el párrafo primero se centrará principalmente en los servicios de TIC prestados por el proveedor tercero esencial de servicios de TIC que sustenten funciones esenciales o importantes de las entidades financieras. Cuando sea necesario para abordar todos los riesgos pertinentes, dicha evaluación abarcará además los servicios de TIC que sustenten funciones distintas de aquellas que son esenciales o importantes.

3. La evaluación a la que se refiere el apartado 2 abarcará:

a) los requisitos en materia de TIC para garantizar, en particular, la seguridad, la disponibilidad, la continuidad, la escalabilidad y la calidad de los servicios que el proveedor tercero esencial de servicios de TIC presta a las entidades financieras, así como la capacidad para mantener en todo momento unos niveles elevados de disponibilidad, autenticidad, integridad o confidencialidad de los datos;

b) la seguridad física que contribuye a garantizar la seguridad de las TIC, incluida la seguridad de los locales, instalaciones y centros de datos;

c) los procesos de gestión de riesgos, incluidas las políticas de gestión del riesgo relacionado con las TIC, la política de continuidad de la actividad en materia de TIC y los planes de respuesta y recuperación en materia de TIC;

d) los mecanismos de gobernanza, incluida una estructura organizativa con líneas de responsabilidad claras, transparentes y coherentes y normas de rendición de cuentas que permitan la gestión eficaz del riesgo relacionado con las TIC;

e) la determinación, el seguimiento y la rápida notificación a las entidades financieras de los incidentes importantes relacionados con las TIC, la gestión y la resolución de dichos incidentes, en particular de los ciberataques;

f) los mecanismos para la portabilidad de los datos y la portabilidad e interoperabilidad de las aplicaciones, que garanticen el ejercicio efectivo de los derechos de terminación por las entidades financieras;

g) la prueba de los sistemas, las infraestructuras y los controles de TIC;

h) las auditorías de TIC;

i) la aplicación de las normas nacionales e internacionales pertinentes en materia de prestación de sus servicios de TIC a las entidades financieras.

4. Sobre la base de la evaluación a que se refiere el apartado 2, y en coordinación con la Red de Supervisión Conjunta a que se refiere el artículo 34, apartado 1, el supervisor principal adoptará un plan de supervisión particular claro, detallado y motivado en el que se describan los objetivos anuales de supervisión y las principales acciones de supervisión previstas para cada proveedor tercero esencial de servicios de TIC. Dicho plan se comunicará cada año al proveedor tercero esencial de servicios de TIC.

Antes de la adopción del plan de supervisión, el supervisor principal comunicará el proyecto de plan de supervisión al proveedor tercero esencial de servicios de TIC.

Cuando reciba el proyecto de plan de supervisión, el proveedor tercero esencial de servicios de TIC podrá presentar una declaración motivada en un plazo de quince días naturales en la que se exponga el efecto esperado en los clientes que sean entidades excluidas del ámbito de aplicación del presente Reglamento y en la que se planteen, en su caso, soluciones para mitigar los riesgos.

5. Una vez que los planes de supervisión anuales a que se refiere el apartado 4 hayan sido adoptados y notificados a los proveedores terceros esenciales de servicios de TIC, las autoridades competentes podrán adoptar medidas en relación con dichos proveedores solo de acuerdo con el supervisor principal.

Artículo 34

Coordinación operativa entre supervisores principales

1. A fin de garantizar un enfoque coherente de las actividades de supervisión y con vistas a posibilitar estrategias generales de supervisión coordinadas y enfoques operativos y metodologías de trabajo coherentes, los tres supervisores principales nombrados de conformidad con el artículo 31, apartado 1, letra b), crearán una Red de Supervisión Conjunta a fin de coordinarse entre sí en las fases preparatorias y de coordinar la realización de las actividades de supervisión de sus proveedores terceros esenciales de servicios de TIC respectivos, así como en el curso de cualquier línea de actuación que pueda ser necesaria en virtud del artículo 42.

2. A efectos del apartado 1, los supervisores principales elaborarán un protocolo común de supervisión en el que se especifiquen los procedimientos detallados que deberán seguirse para llevar a cabo la coordinación cotidiana y para garantizar intercambios y reacciones rápidos. El protocolo se revisará periódicamente para reflejar las necesidades operativas, en particular la evolución de las disposiciones prácticas de supervisión.

3. Los supervisores principales podrán, de forma *ad hoc*, pedir al BCE y a la ENISA que proporcionen asesoramiento técnico, compartan experiencias prácticas o se sumen a determinadas reuniones de coordinación de la Red de Supervisión Conjunta.

Artículo 35

Facultades del supervisor principal

1. A efectos del desempeño de las funciones establecidas en la presente sección, el supervisor principal dispondrá de las siguientes facultades por lo que respecta a los proveedores terceros esenciales de servicios de TIC:

a) solicitar toda la información y la documentación pertinentes de conformidad con el artículo 37;

b) llevar a cabo investigaciones generales e inspecciones de conformidad con los artículos 38 y 39, respectivamente;

c) una vez finalizadas las actividades de supervisión, solicitar informes en los que se especifiquen las medidas adoptadas o las medidas correctoras aplicadas por los proveedores terceros esenciales de servicios de TIC en relación con las recomendaciones a que se refiere la letra d) del presente apartado;

d) formular recomendaciones sobre los ámbitos a los que se refiere el artículo 33, apartado 3, en particular en relación con lo siguiente:

   i) la aplicación de requisitos o procesos específicos de seguridad y calidad de las TIC, en particular en relación con la instalación de parches, actualizaciones, cifrado y otras medidas de seguridad que el supervisor principal considere pertinentes para garantizar la seguridad, desde el punto de vista de las TIC, de los servicios prestados a las entidades financieras,

   ii) la aplicación de condiciones, incluida su ejecución técnica, a las que deba ajustarse la prestación de servicios de TIC a las entidades financieras por los proveedores terceros esenciales de servicios de TIC, y que el supervisor principal considere pertinentes para impedir que se generen o se amplíen puntos únicos de fallo, o para minimizar el posible impacto sistémico en el sector financiero de la Unión en caso de riesgo de concentración de TIC,

   iii) cualquier subcontratación prevista, en caso de que el supervisor principal considere que toda ulterior subcontratación, incluidos los acuerdos de subcontratación que los proveedores terceros esenciales de servicios de TIC prevean celebrar con proveedores terceros de servicios de TIC o con subcontratistas de TIC establecidos en un tercer país, puede ocasionar riesgos para la prestación de servicios por la entidad financiera, o riesgos para la estabilidad financiera, basándose en el examen de la información recabada de conformidad con los artículos 37 y 38,

   iv) abstenerse de celebrar un acuerdo adicional de subcontratación, cuando se cumplan todas las condiciones siguientes:

      — que el subcontratista previsto sea un proveedor tercero de servicios de TIC o un subcontratista de TIC establecido en un tercer país,

      — que la subcontratación se refiera a las funciones esenciales o importantes de la entidad financiera, y

— que el supervisor principal considere que el recurso a tal subcontratación plantea un riesgo claro y grave para la estabilidad financiera de la Unión o para las entidades financieras, también para la capacidad de estas últimas de cumplir los requisitos de supervisión.

A efectos del inciso iv) de la presente letra, los proveedores terceros de servicios de TIC, utilizando la plantilla a que se refiere el artículo 41, apartado 1, letra b), transmitirán la información relativa a la subcontratación al supervisor principal.

2. En el ejercicio de las facultades a que se refiere el presente artículo, el supervisor principal:

a) garantizará una coordinación periódica en el seno de la Red de Supervisión Conjunta y, en particular, perseguirá enfoques coherentes, según proceda, por lo que respecta a la supervisión de los proveedores terceros esenciales de servicios de TIC;

b) tendrá debidamente en cuenta el marco establecido por la Directiva (UE) 2022/2555 y, cuando sea necesario, consultará a las autoridades competentes pertinentes designadas o establecidas de conformidad con dicha Directiva, con el fin de evitar la duplicación de medidas técnicas y organizativas que podrían aplicarse a los proveedores terceros esenciales de servicios de TIC en virtud de dicha Directiva;

c) tratará de minimizar, en la medida de lo posible, el riesgo de perturbación de los servicios prestados por proveedores terceros esenciales de servicios de TIC a clientes que sean entidades excluidas del ámbito de aplicación del presente Reglamento.

3. El supervisor principal consultará al Foro de Supervisión antes de ejercer las facultades a que se refiere el apartado 1.

Antes de formular recomendaciones de conformidad con el apartado 1, letra d), el supervisor principal brindará al proveedor tercero de servicios de TIC la oportunidad de facilitar, en un plazo de treinta días naturales, información pertinente que exponga el efecto previsto en los clientes que sean entidades excluidas del ámbito de aplicación del presente Reglamento y, cuando proceda, que plantee soluciones para mitigar los riesgos.

4. El supervisor principal informará a la Red de Supervisión Conjunta del resultado del ejercicio de las facultades a que se refiere el apartado 1, letras a) y b). El supervisor principal transmitirá, sin demora indebida, los informes a que se refiere el apartado 1, letra c), a la Red de Supervisión Conjunta y a las autoridades competentes de las entidades financieras que utilicen los servicios de TIC de dicho proveedor tercero esencial de servicios de TIC.

5. Los proveedores terceros esenciales de servicios de TIC cooperarán de buena fe con el supervisor principal y lo asistirán en el desempeño de sus tareas.

6. En caso de incumplimiento total o parcial de las medidas cuya adopción se exigió en virtud del ejercicio de las facultades con arreglo al apartado 1, letras a), b) y c), y tras la expiración de un plazo de al menos treinta días naturales a partir de la fecha en que el proveedor tercero esencial de servicios de TIC haya recibido la notificación de las medidas de que se trate, el supervisor principal adoptará una decisión por la que se imponga una multa coercitiva para empujar al proveedor tercero esencial de servicios de TIC a cumplir dichas medidas.

7. La multa coercitiva a que se refiere el apartado 6 se impondrá diariamente hasta que se logre el cumplimiento y por un período máximo de seis meses a partir de la notificación de la decisión de imponer una multa coercitiva al proveedor tercero esencial de servicios de TIC.

8. El importe de la multa coercitiva, calculado a partir de la fecha establecida en la decisión por la que se imponga dicha multa, será de hasta un 1 % del volumen de negocios diario medio a escala mundial del proveedor tercero esencial de servicios de TIC en el ejercicio precedente. Al determinar el importe de la multa coercitiva, el supervisor principal tendrá en cuenta los siguientes criterios en relación con el incumplimiento de las medidas a que se refiere el apartado 6:

a) la gravedad y la duración del incumplimiento;

b) si el incumplimiento ha sido cometido intencionadamente o por negligencia;

c) el nivel de cooperación del proveedor tercero de servicios de TIC con el supervisor principal.

A efectos del párrafo primero el supervisor principal entablará consultas en el seno de la Red de Supervisión Conjunta a fin de garantizar un enfoque coherente.

9. Las multas coercitivas serán de carácter administrativo y tendrán fuerza ejecutiva. La ejecución forzosa se regirá por las normas de procedimiento civil vigentes en el Estado miembro en cuyo territorio se lleven a cabo las inspecciones y el acceso. Los órganos jurisdiccionales del Estado miembro de que se trate serán competentes para conocer de las denuncias relacionadas con irregularidades en la ejecución. Los importes de las multas coercitivas se asignarán al presupuesto general de la Unión Europea.

10. El supervisor principal hará públicas todas las multas coercitivas que se impongan, a menos que dicha divulgación ponga en grave riesgo los mercados financieros o cause un perjuicio desproporcionado a las partes implicadas.

11. Antes de imponer una multa coercitiva de conformidad con el apartado 6, el supervisor principal ofrecerá a los representantes del proveedor tercero esencial de servicios de TIC objeto del procedimiento la oportunidad de ser oídos en relación con las conclusiones y basará sus decisiones únicamente en las conclusiones acerca de las cuales el proveedor tercero esencial de servicios de TIC objeto del procedimiento haya tenido la oportunidad de formular observaciones.

Los derechos de defensa de las personas objeto del procedimiento estarán garantizados plenamente en el curso del procedimiento. El proveedor tercero esencial de servicios de TIC objeto del procedimiento tendrá derecho a acceder al expediente, a reserva del interés legítimo de otras personas por lo que respecta a la protección de sus secretos comerciales. El derecho de acceso al expediente no se extenderá a la información confidencial ni a los documentos preparatorios internos del supervisor principal.

Artículo 36

Ejercicio de las facultades del supervisor principal fuera de la Unión

1. Cuando los objetivos de supervisión no puedan alcanzarse mediante una interacción con la filial establecida a efectos del artículo 31, apartado 12, o mediante el ejercicio de actividades de supervisión en locales situados en la Unión, el supervisor principal podrá ejercer las facultades a que se refieren las disposiciones siguientes en cualquier local situado en un tercer país que sea propiedad de un proveedor tercero esencial de servicios de TIC o este utilice de cualquier modo para prestar servicios a entidades financieras de la Unión, en relación con sus operaciones, funciones o servicios comerciales, incluidos cualquier oficina, local, terreno, edificio u otra propiedad, de naturaleza administrativa comercial u operativa:

a) el artículo 35, apartado 1, letra a), y

b) el artículo 35, apartado 1, letra b), de conformidad con el artículo 38, apartado 2, letras a), b) y d), y el artículo 39, apartado 1 y apartado 2, letra a).

Las facultades a que se refiere el párrafo primero podrán ejercerse siempre que se cumplan todas las condiciones siguientes:

i) el supervisor principal considera necesaria la realización de una inspección en un tercer país para poder desempeñar plena y eficazmente sus funciones con arreglo al presente Reglamento,

ii) la inspección en un tercer país está directamente relacionada con la prestación de servicios de TIC a entidades financieras de la Unión,

iii) el proveedor tercero esencial de servicios de TIC afectado consiente en que se lleve a cabo una inspección en un tercer país, y

iv) la autoridad pertinente del tercer país de que se trate ha sido oficialmente informada por el supervisor principal y no ha formulado objeciones al respecto.

2. Sin perjuicio de las competencias respectivas de las instituciones de la Unión y de los Estados miembros, a efectos del apartado 1, la ABE, la AEVM o la AESPJ, celebrarán acuerdos de cooperación administrativa con la autoridad pertinente del tercer país a fin de que las inspecciones en el tercer país de que se trate por parte del supervisor principal y su equipo designado para su misión en ese tercer país se puedan realizar de manera fluida. Dichos acuerdos de cooperación no crearán obligaciones jurídicas para la Unión y sus Estados miembros ni impedirán a los Estados miembros y a sus autoridades competentes celebrar acuerdos bilaterales o multilaterales con dichos terceros países y sus autoridades pertinentes.

En dichos acuerdos de cooperación se especificarán, como mínimo, los siguientes elementos:

a) los procedimientos para la coordinación de las actividades de supervisión llevadas a cabo con arreglo al presente Reglamento y de cualquier seguimiento análogo del riesgo de terceros relacionado con las TIC en el sector financiero efectuado por la autoridad pertinente del tercer país de que se trate, incluidos los detalles para transmitir el acuerdo de esta última que permita la realización, por parte del supervisor principal y su equipo designado, de las investigaciones generales y las inspecciones *in situ* a que se refiere el apartado 1, párrafo primero, en el territorio bajo su jurisdicción;

b) el mecanismo para la transmisión de cualquier información pertinente entre la ABE, la AEVM o la AESPJ y la autoridad pertinente del tercer país de que se trate, en particular en relación con la información que el supervisor principal puede solicitar en virtud del artículo 37;

c) los mecanismos para la rápida notificación, por parte de la autoridad pertinente del tercer país de que se trate, a la ABE, la AEVM o la AESPJ, de los casos en que se considere que un proveedor tercero de servicios de TIC establecido en un tercer país y designado como esencial de conformidad con el artículo 31, apartado 1, letra a), ha incumplido los requisitos que está obligado a cumplir en virtud del Derecho aplicable del tercer país de que se trate a la hora de prestar servicios a entidades financieras de dicho tercer país, así como de las medidas correctoras y las sanciones aplicadas;

d) la transmisión periódica de información actualizada sobre la evolución en materia de regulación o supervisión en relación con el seguimiento del riesgo de terceros relacionado con las TIC de las entidades financieras del tercer país de que se trate;

e) los detalles para permitir, en caso necesario, la participación de un representante de la autoridad pertinente del tercer país en las inspecciones realizadas por el supervisor principal y el equipo designado.

3. Cuando no pueda llevar a cabo fuera de la Unión las actividades de supervisión a que se refieren los apartados 1 y 2, el supervisor principal deberá:

a) ejercer sus facultades con arreglo al artículo 35 basándose en todos los datos y documentos de que disponga;

b) documentar y explicar cualquier consecuencia de su incapacidad para llevar a cabo las actividades de supervisión previstas a que se refiere el presente artículo.

En las recomendaciones del supervisor principal formuladas en virtud del artículo 35, apartado 1, letra d), se tendrán en cuenta las posibles consecuencias a que se refiere la letra b) del presente apartado.

Artículo 37

Solicitud de información

1. El supervisor principal, mediante simple solicitud o mediante decisión, podrá exigir a los proveedores terceros esenciales de servicios de TIC que faciliten cuanta información le sea necesaria para desempeñar sus funciones con arreglo al presente Reglamento, incluidos todos los documentos comerciales u operativos, contratos, pólizas, documentación, informes de auditorías de seguridad de las TIC e informes sobre incidentes relacionados con las TIC pertinentes, así como cualquier información relativa a las partes a las que el proveedor tercero esencial de servicios de TIC haya externalizado funciones o actividades operativas.

2. Cuando envíe una simple solicitud de información con arreglo al apartado 1, el supervisor principal:

a) hará referencia al presente artículo como base jurídica de la solicitud;

b) indicará el propósito de la solicitud;

c) especificará la información requerida;

d) fijará el plazo en el que habrá de serle facilitada la información;

e) informará al representante del proveedor tercero esencial de servicios de TIC a quien se solicite la información de que, si bien no está obligado a facilitar esa información, en caso de que responda voluntariamente a la solicitud, la información que facilite no deberá ser incorrecta ni engañosa.

3. Cuando exija mediante decisión que se facilite información con arreglo al apartado 1, el supervisor principal:

a) hará referencia al presente artículo como base jurídica de la solicitud;

b) indicará el propósito de la solicitud;

c) especificará la información requerida;

d) fijará el plazo en el que habrá de serle facilitada la información;

e) indicará las multas coercitivas previstas en el artículo 35, apartado 6, en caso de que no se facilite toda la información exigida o de que tal información no se facilite en el plazo a que se refiere la letra d) del presente apartado;

f) hará constar el derecho de recurrir la decisión ante la Sala de Recurso de la Autoridad Europea de Supervisión y ante el Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia»), de conformidad con los artículos 60 y 61 del Reglamento (UE) n.º 1093/2010, los artículos 60 y 61 del Reglamento (UE) n.º 1094/2010 y los artículos 60 y 61 del Reglamento (UE) n.º 1095/2010.

4. Los representantes de los proveedores terceros esenciales de servicios de TIC facilitarán la información solicitada. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. El proveedor tercero esencial de servicios de TIC seguirá siendo plenamente responsable si la información suministrada es incompleta, incorrecta o engañosa.

5. El supervisor principal remitirá sin demora una copia de la decisión de facilitar información a las autoridades competentes de las entidades financieras que utilicen los servicios de los proveedores terceros esenciales de servicios de TIC pertinentes y a la Red de Supervisión Conjunta.

Artículo 38

Investigaciones generales

1. A fin de desempeñar sus funciones con arreglo al presente Reglamento, el supervisor principal, asistido por el equipo conjunto de examinadores a que se refiere el artículo 40, apartado 1, podrá, cuando sea necesario, llevar a cabo investigaciones de proveedores terceros esenciales de servicios de TIC.

2. El supervisor principal estará facultado para:

a) examinar los registros, datos, procedimientos y cualquier otra documentación pertinente para la realización de su cometido, independientemente del medio utilizado para almacenarlos;

b) hacer u obtener copias certificadas o extractos de dichos registros, datos, procedimientos documentados y cualquier otra documentación;

c) convocar a los representantes del proveedor tercero esencial de servicios de TIC para que den explicaciones orales o escritas sobre los hechos o documentos que guarden relación con el objeto y el propósito de la investigación, y registrar las respuestas;

d) entrevistar a cualquier otra persona física o jurídica que acepte ser entrevistada a fin de recabar información relacionada con el objeto de una investigación;

e) requerir una relación de comunicaciones telefónicas y tráfico de datos.

3. Los agentes y demás personas acreditadas por el supervisor principal para realizar la investigación a que se refiere el apartado 1 ejercerán sus facultades previa presentación de una autorización escrita que especifique el objeto y el propósito de la investigación.

Dicha autorización indicará asimismo las multas coercitivas previstas en el artículo 35, apartado 6, cuando los registros, datos, procedimientos documentados o cualquier otra documentación exigida, o las respuestas a las preguntas formuladas a los representantes del proveedor tercero de servicios de TIC, no se faciliten o sean incompletos.

4. Los representantes de los proveedores terceros esenciales de servicios de TIC estarán obligados a someterse a las investigaciones sobre la base de una decisión del supervisor principal. La decisión precisará el objeto y el propósito de la investigación, las multas coercitivas previstas en el artículo 35, apartado 6, las vías de recurso posibles con arreglo a los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010, así como el derecho a recurrir la decisión ante el Tribunal de Justicia.

5. Con suficiente antelación antes del comienzo de la investigación, el supervisor principal informará de la investigación prevista y de la identidad de las personas acreditadas a las autoridades competentes de las entidades financieras que utilicen los servicios de TIC de dicho proveedor tercero esencial de servicios de TIC.

El supervisor principal comunicará a la Red de Supervisión Conjunta toda la información transmitida en virtud del párrafo primero.

Artículo 39

Inspecciones

1. A efectos del desempeño de sus funciones de conformidad con el presente Reglamento, el supervisor principal, asistido por los equipos conjuntos de examinadores a que se refiere el artículo 40, apartado 1, podrá acceder a cualesquiera locales de uso profesional, terrenos o propiedades de los proveedores terceros de servicios de TIC, como sedes centrales, centros de operaciones y locales secundarios, y realizar en ellos, como fuera de ellos, cuantas inspecciones sean necesarias.

A efectos del ejercicio de las facultades a que se refiere el párrafo primero, el supervisor principal consultará a la Red de Supervisión Conjunta.

2. Los agentes del supervisor principal y demás personas acreditadas por él para llevar a cabo una inspección *in situ* estarán facultados para:

a) acceder a cualquiera de dichos locales, terrenos o propiedades de uso profesional, y

b) precintar cualesquiera de dichos locales de uso profesional, libros o registros durante el tiempo y en la medida necesarios para la inspección.

Los agentes y demás personas acreditadas por el supervisor principal ejercerán sus facultades previa presentación de una autorización escrita en la que se especifiquen el objeto y el propósito de la inspección, así como las multas coercitivas establecidas en el artículo 35, apartado 6, en el supuesto de que los representantes de los proveedores terceros esenciales de servicios de TIC de que se trate no se sometan a la inspección.

3. El supervisor principal informará con suficiente antelación antes del comienzo de la inspección a las autoridades competentes de las entidades financieras que recurran a ese proveedor tercero de servicios de TIC.

4. Las inspecciones abarcarán todo el conjunto de sistemas, redes, dispositivos, información y datos de TIC pertinentes utilizados para la prestación de servicios de TIC a las entidades financieras o que contribuyan a ella.

5. Antes de cualquier inspección *in situ* prevista, el supervisor principal avisará con antelación razonable a los proveedores terceros esenciales de servicios de TIC, a menos que dicho aviso no sea posible debido a una situación de emergencia o de crisis, o que conduzca a una situación en la que la inspección o la auditoría dejarían de ser eficaces.

6. El proveedor tercero esencial de servicios de TIC se someterá a las inspecciones *in situ* ordenadas mediante decisión del supervisor principal. La decisión especificará el objeto y el propósito de la inspección, fijará la fecha de comienzo de la inspección e indicará las multas coercitivas previstas en el artículo 35, apartado 6, las vías de recurso posibles con arreglo a los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010, así como el derecho a recurrir la decisión ante el Tribunal de Justicia.

7. En caso de que los agentes y demás personas acreditadas por el supervisor principal constaten que un proveedor tercero esencial de servicios de TIC se opone a una inspección ordenada en virtud del presente artículo, el supervisor principal informará al proveedor tercero esencial de servicios de TIC de las consecuencias de dicha oposición, entre ellas la posibilidad de que las autoridades competentes de las entidades financieras pertinentes obliguen a las entidades financieras a poner fin a los acuerdos contractuales celebrados con dicho proveedor.

Artículo 40

Supervisión permanente

1. Cuando lleve a cabo actividades de supervisión, en particular investigaciones generales o inspecciones, el supervisor principal estará asistido por un equipo conjunto de examinadores establecido para cada proveedor tercero esencial de servicios de TIC.

2. El equipo conjunto de examinadores a que se refiere el apartado 1 estará compuesto por miembros del personal de:

a) las Autoridades Europeas de Supervisión;

b) las autoridades competentes pertinentes que supervisen a las entidades financieras a las que preste servicios de TIC el proveedor tercero esencial de servicios de TIC;

c) con carácter voluntario, la autoridad nacional competente a que se refiere el artículo 32, apartado 4, letra e);

d) con carácter voluntario, una autoridad nacional competente del Estado miembro en el que esté establecido el proveedor tercero esencial de servicios de TIC.

Los miembros del equipo conjunto de examinadores deberán tener conocimientos especializados en cuestiones del ámbito de las TIC y en materia de riesgo operativo. El equipo conjunto de examinadores trabajará bajo la coordinación de un miembro designado del personal del supervisor principal («coordinador del supervisor principal»).

3. En los tres meses siguientes a la conclusión de una investigación o una inspección, el supervisor principal, previa consulta al Foro de Supervisión, adoptará las recomendaciones que se remitirán al proveedor tercero esencial de servicios de TIC en virtud de las facultades a que se refiere el artículo 35.

4. Las recomendaciones a las que se refiere el apartado 3 se comunicarán inmediatamente al proveedor tercero esencial de servicios de TIC y a las autoridades competentes de las entidades financieras a las que preste servicios de TIC.

Para llevar a cabo las actividades de supervisión, el supervisor principal podrá tener en cuenta cualesquiera certificaciones de terceros e informes de auditoría interna o externa de proveedores terceros de TIC pertinentes facilitados por el proveedor tercero esencial de servicios de TIC.

Artículo 41

Armonización de las condiciones que permiten llevar a cabo las actividades de supervisión

1. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación para especificar:

a) la información que debe facilitar un proveedor tercero de servicios de TIC en la solicitud de inclusión voluntaria para ser designado como esencial con arreglo al artículo 31, apartado 11;

b) el contenido, la estructura y el formato de la información que los proveedores terceros de servicios de TIC deben presentar, divulgar o notificar en virtud del artículo 35, apartado 1, incluida la plantilla para informar sobre los acuerdos de subcontratación;

c) los criterios para determinar la composición del equipo conjunto de examinadores, garantizando una participación equilibrada de los miembros del personal de las Autoridades Europeas de Supervisión y de las autoridades competentes pertinentes, así como su designación, tareas y modalidades de trabajo;

d) los pormenores de la evaluación por las autoridades competentes de las medidas adoptadas por los proveedores terceros esenciales de servicios de TIC en aplicación de las recomendaciones del supervisor principal en virtud del artículo 42, apartado 3.

2. Las Autoridades Europeas de Supervisión presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 17 de julio de 2024.

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el apartado 1 del presente artículo de conformidad con el procedimiento establecido en los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º 1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º 1095/2010.

Artículo 42

Seguimiento por las autoridades competentes

1. En el plazo de sesenta días naturales a partir de la recepción de las recomendaciones emitidas por el supervisor principal en virtud del artículo 35, apartado 1, letra d), los proveedores terceros esenciales de servicios de TIC notificarán al supervisor principal si tienen intención de seguir dichas recomendaciones o facilitarán una explicación razonada de los motivos por los que no lo van a hacer. El supervisor principal transmitirá inmediatamente esta información a las autoridades competentes de las entidades financieras de que se trate.

2. Cuando un proveedor tercero esencial de servicios de TIC no presente su notificación al supervisor principal de conformidad con el apartado 1 o cuando la explicación facilitada por el proveedor tercero esencial de servicios de TIC no se considere suficiente, el supervisor principal lo divulgará públicamente. La información publicada revelará la identidad del proveedor tercero esencial de servicios de TIC, así como información sobre el tipo y la naturaleza del incumplimiento. Dicha información se limitará a lo que sea pertinente y proporcionado para garantizar la concienciación del público, a menos que dicha divulgación causare un perjuicio desproporcionado a las partes implicadas o pueda comprometer gravemente el correcto funcionamiento y la integridad de los mercados financieros o la estabilidad del conjunto o de una parte del sistema financiero de la Unión.

El supervisor principal notificará dicha divulgación pública al proveedor tercero de servicios de TIC.

3. Las autoridades competentes informarán a las entidades financieras pertinentes acerca de los riesgos señalados en las recomendaciones a los proveedores terceros esenciales de servicios de TIC de conformidad con el artículo 35, apartado 1, letra d).

Al gestionar el riesgo de terceros relacionado con las TIC, las entidades financieras tendrán en cuenta los riesgos a que se refiere el párrafo primero.

4. Cuando una autoridad competente considere que una entidad financiera no tiene en cuenta o no aborda suficientemente en su gestión del riesgo de terceros relacionado con las TIC los riesgos específicos señalados en las recomendaciones, notificará a la entidad financiera la posibilidad de adoptar una decisión, en el plazo de sesenta días naturales a partir de la recepción de dicha notificación, en virtud del apartado 6, en ausencia de disposiciones contractuales adecuadas destinadas a hacer frente a dichos riesgos.

5. Cuando se reciban los informes a que se refiere el artículo 35, apartado 1, letra c), y antes de tomar la decisión a que se refiere el apartado 6 del presente artículo, las autoridades competentes podrán, de forma voluntaria, consultar a las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555, responsables de la supervisión de una entidad esencial o importante sujeta a dicha Directiva, que haya sido designada como proveedor tercero esencial de servicios de TIC.

6. Como último recurso, tras la notificación y, si procede, tras la consulta establecidas en los apartados 4 y 5 del presente artículo, las autoridades competentes podrán, de conformidad con el artículo 50, tomar la decisión de exigir a las entidades financieras que suspendan temporalmente, de manera parcial o total, el uso o la implantación de un servicio prestado por el proveedor tercero esencial de servicios de TIC hasta que se hayan abordado los riesgos mencionados en las recomendaciones dirigidas a los proveedores terceros esenciales de servicios de TIC. En caso necesario, podrán exigir a las entidades financieras que pongan fin, en parte o en su totalidad, a los acuerdos contractuales pertinentes celebrados con los proveedores terceros esenciales de servicios de TIC.

7. Cuando un proveedor tercero esencial de servicios de TIC se niegue a seguir las recomendaciones sobre la base de un enfoque distinto del recomendado por el supervisor principal y dicho enfoque pueda repercutir negativamente en un gran número de entidades financieras o en una parte considerable del sector financiero, y las advertencias individuales emitidas por las autoridades competentes no hayan dado lugar a enfoques sistemáticos que mitiguen el posible riesgo para la estabilidad financiera, el supervisor principal podrá, previa consulta al Foro de Supervisión, emitir dictámenes no vinculantes y no públicos a las autoridades competentes, a fin de promover medidas de seguimiento en materia de supervisión sistemáticas y convergentes, según proceda.

8. Cuando se reciban los informes a que se refiere el artículo 35, apartado 1, letra c), las autoridades competentes, al tomar la decisión a que se refiere el apartado 6 del presente artículo, tendrán en cuenta el tipo y la magnitud del riesgo no abordado por el proveedor tercero esencial de servicios de TIC, así como la gravedad del incumplimiento, considerando los siguientes criterios:

a) la gravedad y la duración del incumplimiento;

b) si el incumplimiento ha puesto de manifiesto deficiencias graves en los procedimientos, los sistemas de gestión, la gestión de riesgos y los controles internos del proveedor tercero esencial de servicios de TIC;

c) si el incumplimiento ha facilitado o provocado la comisión de un delito financiero o este último le es imputable de cualquier otro modo;

d) si el incumplimiento ha sido cometido intencionadamente o por negligencia;

e) si la suspensión o la terminación de los acuerdos contractuales supone un riesgo para la continuidad de las operaciones comerciales de la entidad financiera, pese a los esfuerzos de esta por evitar perturbaciones en la prestación de sus servicios;

f) cuando proceda, el dictamen, solicitado voluntariamente de conformidad con el apartado 5 del presente artículo, de las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555, responsables de la supervisión de una entidad esencial o importante sujeta a dicha Directiva, que haya sido designada como proveedor tercero esencial de servicios de TIC.

Las autoridades competentes concederán a las entidades financieras el tiempo necesario para que puedan adaptar los acuerdos contractuales con proveedores terceros esenciales de servicios de TIC a fin de evitar efectos perjudiciales en su resiliencia operativa digital y que puedan implantar las estrategias de salida y los planes de transición a que se refiere el artículo 28.

9. La decisión a que se refiere el apartado 6 del presente artículo se notificará a los miembros del Foro de Supervisión a que se refiere el artículo 32, apartado 4, letras a), b) y c), y a la Red de Supervisión Conjunta.

Los proveedores terceros esenciales de servicios de TIC afectados por las decisiones establecidas en el apartado 6 cooperarán plenamente con las entidades financieras perjudicadas, en particular en el contexto del proceso de suspensión o terminación de sus acuerdos contractuales.

10. Las autoridades competentes informarán periódicamente al supervisor principal sobre los enfoques y las medidas adoptados en el desempeño de sus tareas de supervisión en relación con las entidades financieras, así como sobre los acuerdos contractuales celebrados por las entidades financieras cuando los proveedores terceros esenciales de servicios de TIC no hayan refrendado en parte o en su totalidad las recomendaciones que les hayan sido formuladas por el supervisor principal.

11. El supervisor principal podrá, previa solicitud, proporcionar aclaraciones adicionales acerca de las recomendaciones formuladas para orientar a las autoridades competentes sobre las medidas de seguimiento.

Artículo 43

Tasas de supervisión

1. El supervisor principal, de conformidad con el acto delegado a que se refiere el apartado 2 del presente artículo, cobrará a los proveedores terceros esenciales de servicios de TIC unas tasas que cubran por completo los gastos que deba asumir el supervisor principal para la realización de las tareas de supervisión en virtud del presente Reglamento, incluido el reembolso de cualquier coste que pueda derivarse del trabajo realizado por el equipo conjunto de examinadores a que se refiere el artículo 40, así como los costes del asesoramiento facilitado por los expertos independientes a que se refiere el artículo 32, apartado 4, párrafo segundo, en relación con los asuntos que forman parte del ámbito de competencia de las actividades directas de supervisión.

El importe de las tasas cobradas a un proveedor tercero esencial de servicios de TIC cubrirá todos los costes derivados de la ejecución de las obligaciones establecidas en la presente sección y será proporcional a su volumen de negocios.

2. Se otorgan a la Comisión los poderes para adoptar un acto delegado con arreglo al artículo 57 por el que se complete el presente Reglamento mediante la determinación del importe de las tasas y las modalidades de pago, a más tardar el 17 de julio de 2024.

Artículo 44

Cooperación internacional

1. Sin perjuicio de lo dispuesto en el artículo 36, la ABE, la AEVM y la AESPJ podrán, de conformidad con el artículo 33 del Reglamento (UE) n.º 1093/2010, el artículo 33 del Reglamento (UE) n.º 1095/2010 y el artículo 33 del Reglamento (UE) n.º 1094/2010, celebrar acuerdos administrativos con las autoridades de regulación y supervisión de terceros países para fomentar la cooperación internacional en materia de riesgo de terceros relacionado con las TIC en diferentes sectores financieros, en particular mediante el desarrollo de buenas prácticas para la evaluación de los procedimientos y controles en materia de gestión del riesgo relacionado con las TIC, las medidas paliativas y las respuestas a los incidentes.

2. Las Autoridades Europeas de Supervisión, a través del Comité Mixto, presentarán cada cinco años al Parlamento Europeo, al Consejo y a la Comisión un informe confidencial conjunto en el que se resuman las conclusiones de los debates pertinentes mantenidos con las autoridades de terceros países a que se refiere el apartado 1, centrándose en la evolución del riesgo de terceros relacionado con las TIC y sus implicaciones para la estabilidad financiera, la integridad del mercado, la protección de los inversores y el funcionamiento del mercado interior.

CAPÍTULO VI

Acuerdos de intercambio de información

Artículo 45

Acuerdos de intercambio de información en relación con información e inteligencia sobre ciberamenazas

1. Las entidades financieras podrán intercambiar entre sí información e inteligencia sobre ciberamenazas, incluidos indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, en la medida en que dicho intercambio de información e inteligencia:

a) tenga por objeto mejorar la resiliencia operativa digital de las entidades financieras, en particular mediante la concienciación en relación con las ciberamenazas, la limitación o la desactivación de la capacidad de propagación de las ciberamenazas, el apoyo a las capacidades defensivas, las técnicas de detección de amenazas, las estrategias de mitigación o las fases de respuesta y recuperación;

b) tenga lugar dentro de comunidades de entidades financieras de confianza;

c) se realice mediante acuerdos de intercambio de información que protejan el carácter potencialmente sensible de la información compartida y se rijan por normas de conducta que respeten plenamente el secreto comercial, la protección de los datos personales de conformidad con el Reglamento (UE) 2016/679 y las directrices sobre política de competencia.

2. A efectos de lo dispuesto en el apartado 1, letra c), en los acuerdos de intercambio de información se definirán las condiciones de participación y, en su caso, se establecerán los detalles relativos a la participación de las autoridades públicas y a la calidad en la que estas podrán asociarse a dichos acuerdos, los detalles relativos a la participación de los proveedores terceros de servicios de TIC y los relativos a los elementos operativos, incluido el uso de plataformas informáticas especializadas.

3. Las entidades financieras notificarán a las autoridades competentes su participación en los acuerdos de intercambio de información a que se refiere el apartado 1 en el momento en que se valide su incorporación a ellos o, en su caso, el cese de su participación, una vez que se haga efectivo.

CAPÍTULO VII

Autoridades competentes

Artículo 46

Autoridades competentes

Sin perjuicio de las disposiciones relativas al marco de supervisión de los proveedores terceros esenciales de servicios de TIC a que se refiere el capítulo V, sección II, del presente Reglamento, el cumplimiento del presente Reglamento será garantizado por las siguientes autoridades competentes de conformidad con las facultades otorgadas por los respectivos actos jurídicos:

a) en lo que respecta a las entidades de crédito y a las entidades exentas en virtud de la Directiva 2013/36/UE, la autoridad competente designada de conformidad con el artículo 4 de dicha Directiva, y en lo que respecta a las entidades de crédito consideradas como significativas de conformidad con el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013, el BCE de conformidad con las competencias y funciones conferidas por dicho Reglamento;

b) en lo que respecta a las entidades de pago, también las entidades de pago exentas en virtud de la Directiva (UE) 2015/2366, las entidades de dinero electrónico, también las exentas en virtud de la Directiva 2009/110/CE y los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la Directiva (UE) 2015/2366, la autoridad competente designada de conformidad con el artículo 22 de la Directiva (UE) 2015/2366;

c) en lo que respecta a las empresas de servicios de inversión, la autoridad competente designada de conformidad con el artículo 4 de la Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo ([38]);

d) en lo que respecta a los proveedores de servicios de criptoactivos autorizados en virtud del Reglamento relativo a los mercados de criptoactivos y los emisores de fichas referenciadas a activos, la autoridad competente designada de conformidad con las disposiciones pertinentes de dicho Reglamento;

e) en lo que respecta a los depositarios centrales de valores, la autoridad competente designada de conformidad con el artículo 11 del Reglamento (UE) n.º 909/2014;

f) en lo que respecta a las entidades de contrapartida central, la autoridad competente designada de conformidad con el artículo 22 del Reglamento (UE) n.º 648/2012;

g) en lo que respecta a los centros de negociación y los proveedores de servicios de suministro de datos, la autoridad competente designada de conformidad con el artículo 67 de la Directiva 2014/65/UE y la autoridad competente según se define en el artículo 2, apartado 1, punto 18, del Reglamento (UE) n.º 600/2014;

h) en lo que respecta a los registros de operaciones, la autoridad competente designada de conformidad con el artículo 22 del Reglamento (UE) n.º 648/2012;

i) en lo que respecta a los gestores de fondos de inversión alternativos, la autoridad competente designada de conformidad con el artículo 44 de la Directiva 2011/61/UE;

j) en lo que respecta a las sociedades de gestión, la autoridad competente designada de conformidad con el artículo 97 de la Directiva 2009/65/CE;

k) en lo que respecta a las empresas de seguros y de reaseguros, la autoridad competente designada de conformidad con el artículo 30 de la Directiva 2009/138/CE;

l) en lo que respecta a los intermediarios de seguros, de reaseguros y de seguros complementarios, la autoridad competente designada de conformidad con el artículo 12 de la Directiva (UE) 2016/97;

m) en lo que respecta a los fondos de pensiones de empleo, la autoridad competente designada de conformidad con el artículo 47 de la Directiva (UE) 2016/2341;

n) en lo que respecta a las agencias de calificación crediticia, la autoridad competente designada de conformidad con el artículo 21 del Reglamento (CE) n.º 1060/2009;

o) en lo que respecta a los administradores de índices de referencia cruciales, la autoridad competente designada de conformidad con los artículos 40 y 41 del Reglamento (UE) 2016/1011;

([38]) Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativa a la supervisión prudencial de las empresas de servicios de inversión, y por la que se modifican las Directivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE y 2014/65/UE (DO L 314 de 5.12.2019, p. 64).

p) en lo que respecta a los proveedores de servicios de financiación participativa, la autoridad competente designada de conformidad con el artículo 29 del Reglamento (UE) 2020/1503;

q) en lo que respecta a los registros de titulizaciones, la autoridad competente designada de conformidad con el artículo 10 y el artículo 14, apartado 1, del Reglamento (UE) 2017/2402.

Artículo 47

Cooperación con las estructuras y autoridades establecidas por la Directiva (UE) 2022/2555

1. A fin de fomentar la cooperación y permitir los intercambios en materia de supervisión entre las autoridades competentes designadas de conformidad con el presente Reglamento y el Grupo de Cooperación establecido por el artículo 14 de la Directiva (UE) 2022/2555, las Autoridades Europeas de Supervisión y las autoridades competentes podrán participar en las actividades del Grupo de Cooperación en asuntos que atañan a sus actividades en materia de supervisión en relación con las entidades financieras. Las Autoridades Europeas de Supervisión y las autoridades competentes podrán solicitar ser invitadas a participar en las actividades del Grupo de Cooperación en asuntos relativos a las entidades esenciales o importantes sujetas a la Directiva (UE) 2022/2555 que también hayan sido designadas como proveedores terceros esenciales de servicios de TIC en virtud del artículo 31 del presente Reglamento.

2. En su caso, las autoridades competentes podrán consultar y compartir información con los puntos de contacto únicos y los CSIRT designados o establecidos de conformidad con la Directiva (UE) 2022/2555.

3. En su caso, las autoridades competentes podrán solicitar cualquier tipo de asesoramiento y asistencia técnicos pertinentes a las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555 y establecer acuerdos de cooperación para hacer posible el establecimiento de mecanismos de coordinación eficaces y rápidos.

4. Los acuerdos a que se refiere el apartado 3 del presente artículo podrán, entre otros aspectos, especificar los procedimientos para la coordinación de las actividades de supervisión y vigilancia en relación con las entidades esenciales o importantes sujetas a la Directiva (UE) 2022/2555 que hayan sido designadas proveedores terceros esenciales de servicios de TIC en virtud del artículo 31 del presente Reglamento, también en lo relativo a la realización, con arreglo al Derecho nacional, de investigaciones e inspecciones *in situ*, así como a los mecanismos para el intercambio de información entre las autoridades competentes con arreglo al presente Reglamento y las autoridades competentes designadas o establecidas de conformidad con dicha Directiva, que incluye el acceso a la información solicitada por estas últimas.

Artículo 48

Cooperación entre autoridades

1. Las autoridades competentes cooperarán estrechamente entre ellas y, cuando proceda, con el supervisor principal.

2. Las autoridades competentes y el supervisor principal compartirán oportunamente toda la información pertinente relativa a los proveedores terceros esenciales de servicios de TIC que sea necesaria para el desempeño de sus respectivas obligaciones con arreglo al presente Reglamento, en particular en relación con los riesgos detectados, los enfoques y las medidas adoptadas como parte de las tareas de supervisión del supervisor principal.

Artículo 49

Ejercicios, comunicación y cooperación intersectoriales en el ámbito financiero

1. Las Autoridades Europeas de Supervisión, a través del Comité Mixto y en colaboración con las autoridades competentes, las autoridades de resolución a que se refiere el artículo 3 de la Directiva 2014/59/UE, el BCE, la Junta Única de Resolución con respecto a la información relativa a las entidades incluidas en el ámbito de aplicación del Reglamento (UE) n.º 806/2014, la JERS y la ENISA, en su caso, podrán establecer mecanismos que permitan compartir prácticas eficaces entre todos los sectores financieros a fin de mejorar la conciencia situacional y detectar las vulnerabilidades y los riesgos cibernéticos comunes a los diversos sectores.

Podrán organizar ejercicios de gestión de crisis y contingencia que incluyan escenarios de ciberataques con el fin de desarrollar los canales de comunicación y hacer posible gradualmente una respuesta coordinada eficaz a escala de la Unión en caso de que se produzca un incidente grave relacionado con las TIC de alcance transfronterizo o una amenaza conexa que tenga un impacto sistémico en el sector financiero de la Unión en su conjunto.

Dichos ejercicios también podrán someter a prueba, en su caso, las dependencias del sector financiero con respecto a otros sectores económicos.

2. Las autoridades competentes, las Autoridades Europeas de Supervisión y el BCE cooperarán estrechamente entre sí e intercambiarán información para el desempeño de sus obligaciones en virtud de los artículos 47 a 54. Coordinarán estrechamente sus actividades de supervisión con el fin de detectar y reparar las infracciones del presente Reglamento, establecer y promover buenas prácticas, facilitar la colaboración, fomentar la coherencia en la interpretación y proporcionar evaluaciones entre países y territorios en caso de desacuerdo.

Artículo 50

Sanciones administrativas y medidas correctoras

1. Las autoridades competentes dispondrán de todas las facultades de supervisión, investigación y sanción necesarias para cumplir sus obligaciones con arreglo al presente Reglamento.

2. Las facultades a que se refiere el apartado 1 incluirán, como mínimo, las siguientes facultades para:

a) tener acceso a cualquier documento o a los datos bajo cualquier forma que la autoridad competente considere pertinentes para el ejercicio de sus funciones y recibir o procurarse copia de los mismos;

b) realizar investigaciones o inspecciones *in situ*, en las que se llevarán a cabo, entre otras, las siguientes actividades:

   i) convocar a los representantes de las entidades financieras para que den explicaciones orales o escritas sobre los hechos o documentos que guarden relación con el objeto y el propósito de la investigación, y registrar las respuestas,

   ii) entrevistar a cualquier otra persona física o jurídica que acepte ser entrevistada a fin de recabar información relacionada con el objeto de una investigación;

c) exigir medidas correctoras y reparadoras en caso de incumplimiento de los requisitos del presente Reglamento.

3. Sin perjuicio del derecho de los Estados miembros a imponer sanciones penales de conformidad con el artículo 52, los Estados miembros establecerán normas que prevean sanciones administrativas y medidas correctoras adecuadas en caso de infracción del presente Reglamento y garantizarán su aplicación efectiva.

Dichas sanciones y medidas serán eficaces, proporcionadas y disuasorias.

4. Los Estados miembros conferirán a las autoridades competentes la facultad de aplicar al menos las siguientes sanciones administrativas o medidas correctoras en caso de infracción del presente Reglamento:

a) emitir un requerimiento dirigido a la persona física o jurídica que esté infringiendo el presente Reglamento para que ponga fin a su conducta y se abstenga de repetirla;

b) exigir el cese provisional o definitivo de toda práctica o conducta que la autoridad competente considere contraria a las disposiciones del presente Reglamento e impedir la repetición de dicha práctica o conducta;

c) adoptar cualquier tipo de medida, también de carácter pecuniario, para garantizar que las entidades financieras sigan cumpliendo los requisitos legales;

d) exigir, en la medida en que lo permita el Derecho nacional, los registros de tráfico de datos existentes que obren en poder de un operador de telecomunicaciones, cuando existan sospechas fundadas de infracción del presente Reglamento y cuando tales registros puedan ser pertinentes para una investigación de infracciones del presente Reglamento, y

e) publicar avisos, incluidas declaraciones públicas, en las que se indique la identidad de la persona física o jurídica y la naturaleza de la infracción.

5. Cuando el apartado 2, letra c), y el apartado 4 se apliquen a personas jurídicas, los Estados miembros conferirán a las autoridades competentes la facultad de aplicar las sanciones administrativas y las medidas correctoras, según las condiciones que establezca el Derecho nacional, a los miembros del órgano de dirección y a las demás personas físicas que, conforme al Derecho nacional, sean responsables de la infracción.

6. Los Estados miembros garantizará que cualquier decisión de imponer sanciones administrativas o medidas correctivas con arreglo al apartado 2, letra c), esté debidamente motivada y pueda ser objeto de recurso.

Artículo 51

Ejercicio de la facultad de imponer sanciones administrativas y medidas correctoras

1. Las autoridades competentes ejercerán las facultades de imponer las sanciones administrativas y las medidas correctoras a que se refiere el artículo 50 de conformidad con sus ordenamientos jurídicos nacionales, en su caso, de la siguiente manera:

a) directamente;

b) en colaboración con otras autoridades;

c) bajo su responsabilidad, mediante delegación en otras autoridades, o

d) mediante solicitud dirigida a las autoridades judiciales competentes.

2. Al determinar el tipo y el nivel de una sanción administrativa o medida correctora impuesta de conformidad con el artículo 50, las autoridades competentes tendrán en cuenta si la infracción es intencionada o es consecuencia de una negligencia y cualesquiera otras circunstancias pertinentes, entre ellas, en su caso, las siguientes:

a) la importancia, la gravedad y la duración de la infracción;

b) el grado de responsabilidad de la persona física o jurídica responsable de la infracción;

c) la solidez financiera de la persona física o jurídica responsable;

d) la importancia de los beneficios obtenidos o las pérdidas evitadas por la persona física o jurídica responsable, en la medida en que puedan determinarse;

e) las pérdidas causadas a terceros por la infracción, en la medida en que puedan determinarse;

f) el grado de cooperación de la persona física o jurídica responsable con la autoridad competente, sin perjuicio de la obligación de que dicha persona física o jurídica restituya las ganancias obtenidas o las pérdidas evitadas;

g) las infracciones anteriores de la persona física o jurídica responsable.

Artículo 52

Sanciones penales

1. Los Estados miembros podrán decidir no establecer normas que prevean sanciones administrativas o medidas correctoras para las infracciones que estén sujetas a sanciones penales con arreglo a su Derecho nacional.

2. Los Estados miembros que opten por establecer sanciones penales por infracciones del presente Reglamento se asegurarán de que se hayan adoptado las medidas adecuadas para que las autoridades competentes dispongan de todas las facultades necesarias a fin de ponerse en contacto con las autoridades judiciales o las responsables de la fiscalía o de la justicia penal dentro de su jurisdicción, con el fin de obtener información específica relacionada con las investigaciones o procesos penales iniciados por infracciones del presente Reglamento, y de facilitar información del mismo tenor a otras autoridades competentes y a la ABE, la AEVM o la AESPJ, en cumplimiento de su obligación de cooperar a los efectos del presente Reglamento.

Artículo 53

Obligaciones de notificación

Los Estados miembros notificarán las disposiciones legales, reglamentarias y administrativas de aplicación de lo dispuesto en el presente capítulo, incluidas cualesquiera disposiciones pertinentes de Derecho penal, a la Comisión, la AEVM, la ABE y la AESPJ a más tardar el 17 de enero de 2025. Los Estados miembros notificarán sin demora indebida cualquier modificación ulterior de dichas disposiciones a la Comisión, la AEVM, la ABE y la AESPJ.

Artículo 54

Publicación de las sanciones administrativas

1. Las autoridades competentes publicarán en sus sitios web oficiales, sin demora indebida, toda decisión por la que se imponga una sanción administrativa contra la que no haya lugar a recurso tras la notificación de dicha decisión al destinatario de la sanción.

2. La publicación a que se refiere el apartado 1 incluirá información sobre el tipo y la naturaleza de la infracción, la identidad de las personas responsables y las sanciones impuestas.

3. Cuando la autoridad competente, tras una evaluación de cada caso, considere que la publicación de la identidad, cuando se trate de personas jurídicas, o de la identidad y los datos personales, cuando se trate de personas físicas, sería desproporcionada, incluidos los riesgos relacionados con la protección de los datos de carácter personal, pondría en peligro la estabilidad de los mercados financieros o la continuación de una investigación penal en curso, o causaría a la persona afectada daños desproporcionados, en la medida en que estos puedan determinarse, adoptará una de las siguientes soluciones con respecto a la decisión por la que se imponga una sanción administrativa:

a) aplazar su publicación hasta que dejen de existir todos los motivos para no publicarla;

b) publicarla de forma anónima, de conformidad con el Derecho nacional, o

c) abstenerse de publicarla, si las opciones enunciadas en las letras a) y b) se consideran insuficientes para garantizar que la estabilidad de los mercados financieros no corra peligro, o cuando dicha publicación no sea proporcionada con respecto a la moderación de la sanción impuesta.

4. En caso de que se decida publicar una sanción administrativa de forma anónima como se establece en el apartado 3, letra b), podrá aplazarse la publicación de los datos pertinentes.

5. Cuando una autoridad competente publique una decisión que imponga una sanción administrativa que pueda recurrirse ante las autoridades judiciales pertinentes, las autoridades competentes añadirán de forma inmediata en su sitio web oficial dicha información y, con posterioridad, cualquier información ulterior relacionada sobre el resultado del recurso. Se publicará asimismo cualquier resolución judicial que anule una decisión que imponga una sanción administrativa.

6. Las autoridades competentes garantizarán que toda publicación a que se hace referencia en los apartados 1 a 4 permanezca en su sitio web oficial únicamente durante el período de tiempo necesario a los efectos del presente artículo. Este período no excederá de cinco años a partir de su publicación.

Artículo 55

Secreto profesional

1. Toda información confidencial recibida, intercambiada o transmitida en virtud del presente Reglamento estará sujeta a las condiciones de secreto profesional establecidas en el apartado 2.

2. La obligación de secreto profesional se aplicará a todas las personas que trabajen o hayan trabajado para las autoridades competentes en virtud del presente Reglamento o para cualquier otra autoridad u organismo del mercado o persona física o jurídica en los que aquellas hayan delegado sus facultades, incluidos los auditores y expertos contratados por ellas.

3. La información sujeta al secreto profesional, incluido el intercambio de información entre las autoridades competentes con arreglo al presente Reglamento y las autoridades competentes designadas o establecidas de conformidad con la Directiva (UE) 2022/2555, no se divulgará a ninguna otra persona o autoridad, salvo en virtud del Derecho de la Unión o nacional.

4. Toda la información intercambiada por las autoridades competentes en virtud del presente Reglamento y referida a las condiciones comerciales u operativas, así como a otros asuntos de tipo económico o personal, se considerará confidencial y estará amparada por el secreto profesional, salvo cuando la autoridad competente declare, en el momento de su comunicación, que la información puede ser revelada o esta revelación resulte necesaria en el marco de un procedimiento judicial.

Artículo 56

Protección de datos

1. Las Autoridades Europeas de Supervisión y las autoridades competentes solo estarán autorizadas a tratar datos personales cuando sea necesario para el cumplimiento de sus respectivas obligaciones y funciones en virtud del presente Reglamento, en particular en lo que respecta a la investigación, inspección, solicitud de información, comunicación, publicación, evaluación, verificación, evaluación y elaboración de planes de supervisión. Los datos personales serán tratados de conformidad con el Reglamento (UE) 2016/679 o con el Reglamento (UE) 2018/1725, según corresponda.

2. Salvo cuando se disponga otra cosa en otros actos sectoriales, los datos personales a que se refiere el apartado 1 se conservarán hasta el cumplimiento de las obligaciones aplicables en materia de supervisión y, en cualquier caso, durante un período máximo de quince años, salvo en caso de procedimientos judiciales pendientes que requieran conservar dichos datos durante más tiempo.

CAPÍTULO VIII

Actos delegados

Artículo 57

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 los actos delegados a que se refieren el artículo 31, apartado 6, y el artículo 43, apartado 2, se otorgan a la Comisión por un período de cinco años a partir del 17 de enero de 2024. La Comisión elaborará un informe sobre la delegación de poderes a más tardar nueve meses antes de que finalice el período de cinco años. La delegación de poderes se prorrogará tácitamente por períodos de idéntica duración, excepto si el Parlamento Europeo o el Consejo se oponen a dicha prórroga a más tardar tres meses antes del final de cada período.

3. La delegación de poderes mencionada en el artículo 31, apartado 6, y en el artículo 43, 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. En cuanto la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 31, apartado 6, y del artículo 43, apartado 2, entrarán en vigor únicamente si, en un plazo de tres 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 tres meses a iniciativa del Parlamento Europeo o del Consejo.

CAPÍTULO IX

Disposiciones transitorias y finales

Sección I

Artículo 58

Cláusula de revisión

1. A más tardar el 17 de enero de 2028, la Comisión, previa consulta a las Autoridades Europeas de Supervisión y la JERS, en su caso, llevará a cabo una revisión y presentará al Parlamento Europeo y al Consejo un informe, acompañado, en su caso, de una propuesta legislativa. La revisión incluirá, como mínimo, lo siguiente:

a) los criterios para la designación de proveedores terceros esenciales de servicios de TIC de conformidad con el artículo 31, apartado 2;

b) el carácter voluntario de la notificación de ciberamenazas importantes a que se refiere el artículo 19;

c) el régimen a que se refiere el artículo 31, apartado 12, y las competencias del supervisor principal previstas en el artículo 35, apartado 1, letra d), inciso iv), primer guion, con vistas a evaluar la eficacia de dichas disposiciones en lo que respecta a garantizar una supervisión eficaz de los proveedores terceros esenciales de servicios de TIC establecidos en un tercer país, y la necesidad de establecer una filial en la Unión.

   A efectos del párrafo primero de la presente letra, la revisión incluirá un análisis del régimen a que se refiere el artículo 31, apartado 12, también en términos de acceso de las entidades financieras de la Unión a los servicios de terceros países y la disponibilidad de dichos servicios en el mercado de la Unión, y tendrá en cuenta la evolución ulterior de los mercados de los servicios cubiertos por el presente Reglamento, la experiencia práctica de las entidades financieras y los supervisores financieros en relación con la aplicación y, en su caso, la supervisión de dicho régimen, así como cualquier novedad pertinente en materia de regulación y supervisión que se produzca a escala internacional;

d) la conveniencia de incluir en el ámbito de aplicación del presente Reglamento a las entidades financieras a que se refiere el artículo 2, apartado 3, letra e), que hagan uso de sistemas automatizados de venta, a la luz de la futura evolución del mercado en lo relativo al uso de dichos sistemas;

e) el funcionamiento y la eficacia de la Red de Supervisión Conjunta a la hora de apoyar la homogeneidad de la supervisión y la eficiencia del intercambio de información en el marco de supervisión.

2. En el contexto de la revisión de la Directiva (UE) 2015/2366, la Comisión evaluará la necesidad de aumentar la ciberresiliencia de los sistemas de pago y las actividades de procesamiento de pagos, así como la conveniencia de ampliar el ámbito de aplicación del presente Reglamento a los operadores de sistemas de pago y a las entidades que participen en actividades de procesamiento de pagos. A la luz de esta evaluación, la Comisión presentará, como parte de la revisión de la Directiva (UE) 2015/2366, un informe al Parlamento Europeo y al Consejo a más tardar el 17 de julio de 2023.

A partir de dicho informe de revisión, y previa consulta a las Autoridades Europeas de Supervisión, el BCE y la JERS, la Comisión podrá presentar, en su caso y como parte de la propuesta legislativa que podrá adoptar en virtud del artículo 108, párrafo segundo, de la Directiva (UE) 2015/2366, una propuesta para garantizar que todos los operadores de sistemas de pago y entidades que participen en actividades de procesamiento de pagos estén sujetos a una supervisión adecuada, teniendo en cuenta al mismo tiempo la supervisión existente por parte de los bancos centrales.

3. A más tardar el 17 de enero de 2026, la Comisión, previa consulta a las Autoridades Europeas de Supervisión y a la Comisión de Organismos Europeos de Supervisión de Auditores, llevará a cabo una revisión y presentará al Parlamento Europeo y al Consejo un informe, acompañado, en su caso, de una propuesta legislativa, sobre la conveniencia de reforzar los requisitos para los auditores legales y sociedades de auditoría en lo relativo a la resiliencia operativa digital, mediante la inclusión en el ámbito de aplicación del presente Reglamento de los auditores legales y las sociedades de auditoría o mediante la modificación de la Directiva 2006/43/CE del Parlamento Europeo y del Consejo ([39]).

Sección II

Modificaciones

Artículo 59

Modificaciones del Reglamento (CE) n.º 1060/2009

El Reglamento (CE) n.º 1060/2009 se modifica como sigue:

1) En el anexo I, sección A, punto 4, el párrafo primero se sustituye por el texto siguiente:

«Las agencias de calificación crediticia dispondrán de procedimientos administrativos y contables adecuados, mecanismos de control interno, técnicas eficaces de valoración del riesgo y mecanismos eficaces de control y salvaguardia para gestionar sus sistemas de TIC de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

2) En el anexo III, el punto 12 se sustituye por el texto siguiente:

«12. Infringe el artículo 6, apartado 2, leído en relación con el anexo I, sección A, punto 4, la agencia de calificación crediticia que no disponga de procedimientos administrativos o contables adecuados, mecanismos de control interno, técnicas eficaces de evaluación del riesgo o mecanismos eficaces de control o salvaguardia para gestionar sus sistemas de TIC de conformidad con el Reglamento (UE) 2022/2554, o que no aplique o mantenga procedimientos de adopción de decisiones o estructuras organizativas según lo prescrito en dicho punto.».

Artículo 60

Modificaciones del Reglamento (UE) n.º 648/2012

El Reglamento (UE) n.º 648/2012 se modifica como sigue:

1) El artículo 26 se modifica como sigue:

a) el apartado 3 se sustituye por el texto siguiente:

«3. Las ECC mantendrán y aplicarán una estructura organizativa que garantice la continuidad y el correcto funcionamiento de la prestación de sus servicios y la realización de sus actividades. Emplearán sistemas, recursos y procedimientos adecuados y proporcionados, incluidos sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).»;

([39]) Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas 78/660/CEE y 83/349/CEE del Consejo y se deroga la Directiva 84/253/CEE del Consejo (DO L 157 de 9.6.2006, p. 87).

b) se suprime el apartado 6.

2) El artículo 34 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. Las ECC establecerán, aplicarán y mantendrán una política adecuada de continuidad de la actividad y un plan de recuperación en caso de catástrofe, que incluirán una política de continuidad de la actividad en materia de TIC y planes de respuesta y recuperación en materia de TIC establecidos e implantados de conformidad con el Reglamento (UE) 2022/2554, destinados a garantizar la preservación de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones.»;

b) en el apartado 3, el párrafo primero se sustituye por el texto siguiente:

«3. A fin de garantizar la aplicación coherente del presente artículo, la AEVM, previa consulta a los miembros del SEBC, elaborará proyectos de normas técnicas reglamentarias en las que se especifiquen el contenido y los requisitos mínimos de la política de continuidad de la actividad y del plan de recuperación en caso de catástrofe, que excluirán la política de continuidad de la actividad y los planes de recuperación en caso de catástrofe en materia de TIC.».

3) En el artículo 56, apartado 3, el párrafo primero se sustituye por el texto siguiente:

«3. A fin de garantizar la aplicación coherente del presente artículo, la AEVM elaborará proyectos de normas técnicas de regulación en las que se especifiquen los pormenores, que no sean los relativos a los requisitos relacionados con la gestión del riesgo relacionado con las TIC, de la solicitud de inscripción a que se refiere el apartado 1.».

4) En el artículo 79, los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Los registros de operaciones detectarán las fuentes de riesgo operativo y las reducirán al mínimo también mediante el desarrollo de sistemas, controles y procedimientos adecuados, incluidos sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2022/2554.

2. Los registros de operaciones establecerán, aplicarán y mantendrán una política adecuada de continuidad de la actividad y un plan de recuperación en caso de catástrofe, que incluirán una política de continuidad de la actividad en materia de TIC y planes de respuesta y recuperación en materia de TIC establecidos de conformidad con el Reglamento (UE) 2022/2554, destinados a garantizar el mantenimiento de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones.».

5) En el artículo 80, se suprime el apartado 1.

6) En el anexo I, la sección II se modifica como sigue:

a) las letras a) y b) se sustituyen por el texto siguiente:

«a) infringe el artículo 79, apartado 1, el registro de operaciones que no detecta las fuentes de riesgo operativo o no reduce al mínimo dicho riesgo mediante el desarrollo de sistemas, controles y procedimientos adecuados, incluidos sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2022/2554;

b) infringe el artículo 79, apartado 2, el registro de operaciones que no establece, aplica y mantiene una política adecuada de continuidad de la actividad y un plan de recuperación en caso de catástrofe establecidos de conformidad con el Reglamento (UE) 2022/2554, destinados a garantizar el mantenimiento de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones;»;

b) se suprime la letra c).

7) El anexo III se modifica como sigue:

a) la sección II se modifica como sigue:

i) la letra c) se sustituye por el texto siguiente:

«c) infringe el artículo 26, apartado 3, la ECC de nivel 2 que no mantiene o aplica una estructura organizativa que garantice la continuidad y el correcto funcionamiento de la prestación de sus servicios y la realización de sus actividades, o que no utiliza sistemas, recursos o procedimientos adecuados y proporcionados, incluidos los sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2022/2554;»,

ii) se suprime la letra f);

b) en la sección III, la letra a) se sustituye por el texto siguiente:

«a) infringe el artículo 34, apartado 1, la ECC de nivel 2 que no establece, aplica o mantiene una política adecuada de continuidad de la actividad y un plan de respuesta y recuperación establecidos con arreglo al Reglamento (UE) 2022/2554, destinados a garantizar la preservación de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones, y que permita como mínimo la recuperación de todas las operaciones en el momento de la perturbación, con objeto de que la ECC pueda seguir operando de manera segura y finalizar la liquidación en la fecha programada;».

Artículo 61

Modificaciones del Reglamento (UE) n.º 909/2014

El artículo 45 del Reglamento (UE) n.º 909/2014 se modifica como sigue:

1) El apartado 1 se sustituye por el texto siguiente:

«1. Los DCV detectarán las fuentes de riesgo operativo, tanto internas como externas, y minimizarán su repercusión también mediante la implantación de herramientas, procesos y políticas en materia de TIC adecuados, establecidos y gestionados de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), así como mediante cualesquiera otros instrumentos, controles y procedimientos adecuados y pertinentes para otros tipos de riesgo operativo, asimismo en relación con todos los sistemas de liquidación de valores que operen.

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

2) Se suprime el apartado 2.

3) Los apartados 3 y 4 se sustituyen por el texto siguiente:

«3. En lo que respecta a los servicios que presten, y en relación con cada sistema de liquidación de valores que exploten, los DCV establecerán, aplicarán y mantendrán una política adecuada de continuidad de la actividad y un plan de recuperación en caso de catástrofe, que incluirá una política de continuidad de la actividad en materia de TIC y planes de respuesta y recuperación en materia de TIC, establecidos de conformidad con el Reglamento (UE) 2022/2554, a fin de garantizar el mantenimiento de sus servicios, la oportuna recuperación de las operaciones y el cumplimiento de las obligaciones del DCV ante acontecimientos que supongan un riesgo importante de perturbación de las operaciones.

4. El plan a que se refiere el apartado 3 deberá prever la recuperación de todas las operaciones y posiciones de los participantes en el momento de la perturbación, con objeto de que los participantes del DCV puedan seguir operando con certeza y finalizar la liquidación en la fecha programada, para lo cual el plan deberá garantizar, en particular, que los sistemas informáticos esenciales puedan reanudar las operaciones a partir del momento de la perturbación, según lo establecido en el artículo 12, apartados 5 y 7, del Reglamento (UE) 2022/2554.».

4) El apartado 6 se sustituye por el texto siguiente:

«6. Los DCV determinarán, controlarán y gestionarán los riesgos que los participantes más importantes de los sistemas de liquidación de valores que gestionan, así como los prestadores de servicios y otros DCV u otras infraestructuras del mercado puedan suponer para su funcionamiento. Facilitarán a las autoridades competentes y pertinentes, a petición de estas, información sobre todo riesgo de este tipo que se detecte. Informarán asimismo sin demora a las autoridades competentes y las autoridades pertinentes de todo incidente operativo que no guarde relación con el riesgo relacionado con las TIC, resultante de tales riesgos.».

5) En el apartado 7, el párrafo primero se sustituye por el texto siguiente:

«7. La AEVM, en estrecha cooperación con los miembros del SEBC, elaborará proyectos de normas técnicas de regulación que especifiquen los riesgos operativos a que se refieren los apartados 1 y 6, que no sean riesgos relacionados con las TIC, los métodos para someter a prueba, afrontar o minimizar tales riesgos, incluidas las políticas de continuidad de la actividad y los planes de recuperación en caso de catástrofe a que se refieren los apartados 3 y 4, y los correspondientes métodos de evaluación.».

Artículo 62

Modificaciones del Reglamento (UE) n.º 600/2014

El Reglamento (UE) n.º 600/2014 se modifica como sigue:

1) El artículo 27 *octies* se modifica como sigue:

a) el apartado 4 se sustituye por el texto siguiente:

«4. Los APA cumplirán los requisitos relativos a la seguridad de las redes y los sistemas de información establecidos en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).»;

b) en el apartado 8, la letra c) se sustituye por el texto siguiente:

«c) los requisitos concretos de organización establecidos en los apartados 3 y 5.».

2) El artículo 27 *nonies* se modifica como sigue:

a) el apartado 5 se sustituye por el texto siguiente:

«5. Los PIC cumplirán los requisitos relativos a la seguridad de las redes y los sistemas de información establecidos en el Reglamento (UE) 2022/2554.»;

b) en el apartado 8, la letra e) se sustituye por el texto siguiente:

«e) los requisitos concretos de organización establecidos en el apartado 4.».

3) El artículo 27 *decies* se modifica como sigue:

a) el apartado 3 se sustituye por el texto siguiente:

«3. Los SIA cumplirán los requisitos relativos a la seguridad de las redes y los sistemas de información establecidos en el Reglamento (UE) 2022/2554.»;

b) en el apartado 5, la letra b) se sustituye por el texto siguiente:

«b) los requisitos concretos de organización establecidos en los apartados 2 y 4.».

Artículo 63

Modificaciones del Reglamento (UE) 2016/1011

En el artículo 6 del Reglamento (UE) 2016/1011 se añade el apartado siguiente:

«6. En lo relativo a los índices de referencia cruciales, el administrador dispondrá de procedimientos administrativos y contables adecuados, mecanismos de control interno, técnicas eficaces de valoración del riesgo y mecanismos eficaces de control y salvaguardia para gestionar sus sistemas de TIC de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

Artículo 64

Entrada en vigor y aplicación

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

Será aplicable a partir del 17 de enero de 2025.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el 14 de diciembre de 2022.

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

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]) — 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 — 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]) — Entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2 — 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 — 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 — 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

DIRECTIVA (UE) 2022/2556 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 14 de diciembre de 2022

por la que se modifican las Directivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 en lo relativo a la resiliencia operativa digital del sector financiero

(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 53, apartado 1, y 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]),

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

Considerando lo siguiente:

(1) La Unión debe afrontar adecuada y exhaustivamente los riesgos digitales que se derivan para todas las entidades financieras de un mayor uso de las tecnologías de la información y la comunicación (TIC) en la prestación y el consumo de servicios financieros, contribuyendo así a la materialización del potencial de las finanzas digitales, desde el punto de vista del impulso de la innovación y el fomento de la competencia en un entorno digital seguro.

(2) Las entidades financieras dependen en gran medida del uso de las tecnologías digitales en sus actividades cotidianas. Es de suma importancia garantizar la resiliencia operativa de sus operaciones digitales frente al riesgo relacionado con las TIC. Esta necesidad se ha vuelto aún más acuciante con el crecimiento en el mercado de las tecnologías de vanguardia, en particular las tecnologías que permiten transferir y almacenar electrónicamente representaciones digitales de valor o derechos utilizando tecnología de registro descentralizado o tecnologías similares («criptoactivos»), así como de los servicios relacionados con dichos activos.

([1]) DO C 343 de 26.8.2021, p. 1.
([2]) DO C 155 de 30.4.2021, p. 38.
([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.

(3) A nivel de la Unión, los requisitos relacionados con la gestión de los riesgos que plantean las TIC para el sector financiero se encuentran actualmente establecidos en las Directivas 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) y (UE) 2016/2341 ([11]) del Parlamento Europeo y del Consejo.

Dichos requisitos son diversos y, en ocasiones, están incompletos. En algunos casos, el riesgo relacionado con las TIC solo se ha abordado implícitamente dentro del riesgo operativo, y en otros casos no se ha abordado en absoluto. Esos problemas deben subsanarse mediante la adopción del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([12]). Por tanto, dichas Directivas deben modificarse para garantizar la coherencia con dicho Reglamento. La presente Directiva adopta una serie de modificaciones que son necesarias para aportar claridad jurídica y coherencia en relación con la aplicación, por parte de las entidades financieras autorizadas y supervisadas de conformidad con dichas Directivas, de diversos requisitos de resiliencia operativa digital que son indispensables en el ejercicio de sus actividades y en la prestación de servicios, garantizando así el buen funcionamiento del mercado interior. Es necesario garantizar la adecuación de dichos requisitos con relación a la evolución del mercado, y al mismo tiempo fomentar la proporcionalidad, en particular por lo que respecta al tamaño de las entidades financieras y a los regímenes específicos a los que están sujetas, con el fin de reducir los costes de conformidad.

(4) En el ámbito de los servicios bancarios, la Directiva 2013/36/UE solo establece actualmente normas generales de gobernanza interna y disposiciones sobre el riesgo operativo que requieren la elaboración de planes de emergencia y de continuidad de la actividad que sirven implícitamente de base para afrontar los riesgos relacionados con las TIC. No obstante, para afrontar los riesgos relacionados con las TIC de forma explícita y clara, deben modificarse los requisitos en materia de planes de emergencia y de continuidad de la actividad para incluir también planes de continuidad de las actividades y planes de respuesta y recuperación referidos al riesgo relacionado con las TIC, de conformidad con los requisitos establecidos en el Reglamento (UE) 2022/2554. Además, el riesgo relacionado con las TIC solo se incluye implícitamente, como parte del riesgo operativo, en el proceso de revisión y evaluación supervisora efectuado por las autoridades competentes, y los criterios para su evaluación se definen actualmente en las Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES), emitidas por la Autoridad Europea de Supervisión (AES) (Autoridad Bancaria Europea o ABE), creada en virtud del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([13]). A fin de aportar claridad

([4]) Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM) (DO L 302 de 17.11.2009, p. 32).

([5]) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1).

([6]) Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) n.º 1060/2009 y (UE) n.º 1095/2010 (DO L 174 de 1.7.2011, p. 1).

([7]) Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

([8]) Directiva 2014/59/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, por la que se establece un marco para la recuperación y la resolución de entidades de crédito y empresas de servicios de inversión, y por la que se modifican la Directiva 82/891/CEE del Consejo, y las Directivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE y 2013/36/UE, y los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 648/2012 del Parlamento Europeo y del Consejo (DO L 173 de 12.6.2014, p. 190).

([9]) 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).

([10]) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35).

([11]) Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2016, relativa a las actividades y la supervisión de los fondos de pensiones de empleo (FPE) (DO L 354 de 23.12.2016, p. 37).

([12]) 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).

([13]) Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12).

jurídica y garantizar que los supervisores bancarios detecten eficazmente el riesgo relacionado con las TIC y vigilen su gestión por parte de las entidades financieras, en consonancia con el nuevo marco sobre la resiliencia operativa digital, debe modificarse también el ámbito de aplicación del proceso de revisión y evaluación supervisora a fin de hacer remisión explícita a los requisitos establecidos en el Reglamento (UE) 2022/2554 y de abarcar, en particular, los riesgos que se hayan puesto de manifiesto en los informes de incidentes graves relacionados con las TIC y en los resultados de las pruebas de resiliencia operativa digital realizadas por las entidades financieras de conformidad con dicho Reglamento.

(5) La resiliencia operativa digital es fundamental para preservar las funciones esenciales y las ramas de actividad principales de una entidad financiera en caso de que se produzca su resolución, y evitar así perturbaciones en la economía real y en el sistema financiero. Los incidentes operativos graves pueden menoscabar la capacidad de una entidad financiera para seguir operando y pueden poner en peligro los objetivos de resolución. Algunos acuerdos contractuales sobre el uso de servicios de TIC son fundamentales para garantizar la continuidad operativa y proporcionar los datos necesarios en caso de resolución. Procede, por tanto, modificar la Directiva 2014/59/UE a fin de ajustarla a los objetivos del marco de la Unión para la resiliencia operativa, con vistas a asegurar que la información relacionada con la resiliencia operativa se tenga en cuenta en el contexto de la planificación de la resolución y la evaluación de la resolubilidad de las entidades financieras.

(6) La Directiva 2014/65/UE establece normas más estrictas en materia del riesgo relacionado con las TIC para las empresas de servicios de inversión y los centros de negociación que están participando en una negociación algorítmica. Se imponen requisitos menos detallados a los servicios de suministro de datos y a los registros de operaciones. Asimismo, la Directiva 2014/65/UE solo hace referencia de forma limitada a los mecanismos de control y salvaguardia de los sistemas informáticos y a la utilización de sistemas, recursos y procedimientos adecuados para garantizar la continuidad y regularidad de los servicios empresariales. Además, dicha Directiva debe armonizarse con el Reglamento (UE) 2022/2554 en lo que se refiere a la continuidad y regularidad en la prestación de servicios de inversión y en la realización de actividades de inversión, la resiliencia operativa, la capacidad de los sistemas de negociación y la eficacia de los mecanismos de continuidad de la actividad y la gestión de riesgos.

(7) La Directiva (UE) 2015/2366 establece normas específicas sobre las medidas de control de la seguridad y mitigación del riesgo relacionado con las TIC a efectos de la obtención de una autorización para prestar servicios de pago. Dichas normas de autorización deben modificarse para adaptarlas al Reglamento (UE) 2022/2554. Además, con el fin de reducir la carga administrativa y evitar la complejidad y la duplicación de los requisitos de notificación, las normas de notificación de incidentes de dicha Directiva deben dejar de aplicarse a los proveedores de servicios de pago regulados por dicha Directiva y sujetos también a lo dispuesto en el Reglamento (UE) 2022/2554, permitiendo así a dichos proveedores de servicios de pago que se beneficien de un mecanismo único, plenamente armonizado, de notificación de incidentes aplicable a todos los incidentes operativos o de seguridad relacionados con los pagos, con independencia de si tales incidentes están relacionados con las TIC.

(8) Las Directivas 2009/138/CE y (UE) 2016/2341 tienen parcialmente en cuenta el riesgo relacionado con las TIC en sus disposiciones generales sobre gobernanza y gestión de riesgos, dejando que determinados requisitos se especifiquen mediante actos delegados, con o sin referencias específicas al riesgo relacionado con las TIC. Del mismo modo, los gestores de fondos de inversión alternativos regulados por la Directiva 2011/61/UE y las sociedades de gestión reguladas por la Directiva 2009/65/CE solo están sujetos a normas muy generales. Por consiguiente, esas Directivas deben adaptarse a los requisitos establecidos en el Reglamento (UE) 2022/2554 en lo que respecta a la gestión de los sistemas y herramientas de TIC.

(9) En muchos casos, ya se han establecido requisitos adicionales en materia del riesgo relacionado con las TIC en actos delegados y de ejecución, adoptados a partir de los proyectos de normas técnicas de regulación y de los proyectos de normas técnicas de ejecución elaborados por la Autoridad Europea de Supervisión competente. Dado que en lo sucesivo, las disposiciones del Reglamento (UE) 2022/2554 constituyen el marco jurídico para el riesgo relacionado con las TIC en el sector financiero, deben modificarse determinadas habilitaciones para adoptar actos delegados y de ejecución contenidas en las Directivas 2009/65/CE, 2009/138/CE, 2011/61/UE y 2014/65/UE para eliminar las disposiciones relativas al riesgo relacionado con las TIC del ámbito de dichas habilitaciones.

(10) Para garantizar una aplicación coherente del nuevo marco para la resiliencia operativa digital del sector financiero, los Estados miembros deben aplicar las disposiciones de Derecho nacional de transposición de la presente Directiva a partir de la fecha de aplicación del Reglamento (UE) 2022/2554.

(11) Las Directivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 fueron adoptadas sobre la base del artículo 53, apartado 1, o del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), o de ambos. Las modificaciones contenidas en la presente Directiva se han incluido en un único acto legislativo, ya que su objeto y las finalidades que persiguen están interconectados. Por consiguiente, la presente Directiva debe adoptarse sobre la base tanto del artículo 53, apartado 1, como del artículo 114 del TFUE.

(12) Dado que los objetivos de la presente Directiva no pueden ser alcanzados de manera suficiente por los Estados miembros, al implicar una armonización de requisitos ya contenidos en otras Directivas, sino que, debido al alcance y los efectos de la acción, pueden 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 dichos objetivos.

(13) De conformidad con la Declaración política conjunta, de 28 de septiembre de 2011, de los Estados miembros y de la Comisión sobre los documentos explicativos ([14]), los Estados miembros se han comprometido a adjuntar a la notificación de las medidas de transposición, cuando esté justificado, uno o varios documentos que expliquen la relación entre los elementos de una directiva y las partes correspondientes de los instrumentos nacionales de transposición. Por lo que respecta a la presente Directiva, el legislador considera que la transmisión de tales documentos está justificada.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Modificaciones de la Directiva 2009/65/CE

El artículo 12 de la Directiva 2009/65/CE se modifica como sigue:

1) En el apartado 1, párrafo segundo, la letra a) se sustituye por el texto siguiente:

«a) cuente con una buena organización administrativa y contable, con mecanismos de control y seguridad para el tratamiento electrónico de datos, también con respecto a redes y sistemas de información establecidos y gestionados de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), así como con procedimientos de control interno adecuados, incluidas, en particular, normas que regulen las transacciones personales de sus empleados o la tenencia o gestión de inversiones en instrumentos financieros con objeto de invertir por cuenta propia, a fin de garantizar, como mínimo, que cada transacción relacionada con el OICVM pueda reconstruirse con arreglo a su origen, las partes que intervengan, su naturaleza y el momento y lugar en que se haya realizado, y que los activos de los OICVM gestionados por la sociedad de gestión se inviertan con arreglo al reglamento del fondo o los documentos constitutivos y a las disposiciones legales vigentes;

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

2) El apartado 3 se sustituye por el texto siguiente:

«3. Sin perjuicio del artículo 116, la Comisión adoptará, mediante actos delegados de conformidad con el artículo 112 *bis*, medidas que especifiquen lo siguiente:

a) los procedimientos y mecanismos a que se refiere el apartado 1, párrafo segundo, letra a), distintos de los procedimientos y mecanismos relacionados con las redes y los sistemas de información;

b) las estructuras y los requisitos organizativos para minimizar los conflictos de intereses a que se refiere el apartado 1, párrafo segundo, letra b).».

([14]) DO C 369 de 17.12.2011, p. 14.

Artículo 2

Modificaciones de la Directiva 2009/138/CE

La Directiva 2009/138/CE se modifica como sigue:

1) En el artículo 41, el apartado 4 se sustituye por el texto siguiente:

«4. Las empresas de seguros y de reaseguros adoptarán medidas razonables para garantizar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de emergencia. A tal fin, las empresas emplearán sistemas, recursos y procedimientos adecuados y proporcionados y, en particular, establecerán y gestionarán redes y sistemas de información de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

2) En el artículo 50, apartado 1, las letras a) y b) se sustituyen por el texto siguiente:

«a) los elementos de los sistemas a que se refiere el artículo 41, el artículo 44, en particular las áreas enumeradas en su apartado 2, y los artículos 46 y 47, distintos de los elementos relativos a la gestión del riesgo relacionado con las tecnologías de la información y la comunicación;

b) las funciones a que se refieren los artículos 44, 46, 47 y 48, distintas de las relacionadas con la gestión del riesgo relacionado con las tecnologías de la información y la comunicación.».

Artículo 3

Modificación de la Directiva 2011/61/UE

El artículo 18 de la Directiva 2011/61/UE se sustituye por el texto siguiente:

«*Artículo 18*

Principios generales

1. Los Estados miembros exigirán que los GFIA empleen en todo momento los recursos humanos y técnicos adecuados y oportunos que precise la correcta gestión de los FIA.

En particular, las autoridades competentes del Estado miembro de origen de cada GFIA exigirán a este, teniendo en cuenta también la naturaleza de los FIA que gestione, que cuente con procedimientos administrativos y contables adecuados, con mecanismos de control y seguridad para el tratamiento electrónico de datos, también con respecto a redes y sistemas de información establecidos y gestionados de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), así como con procedimientos de control interno adecuados, incluidas, en particular, normas que rijan las transacciones personales de sus empleados o la tenencia o gestión de inversiones con objeto de invertir por cuenta propia, a fin de garantizar, como mínimo, que cada transacción relacionada con el FIA pueda reconstruirse por lo que respecta a su origen, los participantes, su naturaleza y el momento y lugar en que se haya realizado, y que los activos de los FIA gestionados por el GFIA se inviertan con arreglo al reglamento o los documentos constitutivos del FIA y a las disposiciones legales vigentes.

2. La Comisión adoptará, mediante actos delegados de conformidad con el artículo 56 y observando las condiciones establecidas en los artículos 57 y 58, medidas que especifiquen los procedimientos y mecanismos a que se refiere el apartado 1 del presente artículo, distintos de los procedimientos y mecanismos relacionados con las redes y los sistemas de información.

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

Artículo 4

Modificaciones de la Directiva 2013/36/UE

La Directiva 2013/36/UE se modifica como sigue:

1) En el artículo 65, apartado 3, letra a), el inciso vi) se sustituye por el texto siguiente:

«vi) terceros a los que las entidades contempladas en los incisos i) a iv) hayan subcontratado funciones o actividades, incluidos los proveedores terceros de servicios de tecnologías de la información y la comunicación (TIC) a que se refiere el capítulo V del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*).

(*) 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 (DO L 333 de 27.12.2022, p. 1).».

2) En el artículo 74, apartado 1, el párrafo primero se sustituye por el texto siguiente:

«Las entidades se dotarán de sólidos mecanismos de gobierno corporativo, incluida una estructura organizativa clara con líneas de responsabilidad bien definidas, transparentes y coherentes, procedimientos eficaces de detección, gestión, control y notificación de los riesgos a los que estén expuestas o puedan estarlo, mecanismos adecuados de control interno, incluidos procedimientos administrativos y contables correctos, redes y sistemas de información establecidos y gestionados de conformidad con el Reglamento (UE) 2022/2554, y políticas y prácticas de remuneración que sean compatibles con una gestión de riesgos adecuada y eficaz y la promuevan.».

3) En el artículo 85, el apartado 2 se sustituye por el texto siguiente:

«2. Las autoridades competentes garantizarán que las entidades dispongan de políticas y planes de emergencia y de continuidad de la actividad adecuados, que incluyan políticas y planes de continuidad de las actividades de TIC y planes de respuesta y recuperación en materia de TIC en relación con la tecnología que utilicen para la comunicación de información, y que esos planes se establezcan, gestionen y pongan a prueba de conformidad con el artículo 11 del Reglamento (UE) 2022/2554, para que las entidades puedan seguir funcionando en caso de perturbaciones graves en su actividad y limiten las pérdidas en que incurran como consecuencia de dichas perturbaciones.».

4) En el artículo 97, apartado 1, se añade la letra siguiente:

«d) los riesgos que se hayan puesto de manifiesto en las pruebas de resiliencia operativa digital efectuadas de conformidad con el capítulo IV del Reglamento (UE) 2022/2554.».

Artículo 5

Modificaciones de la Directiva 2014/59/UE

La Directiva 2014/59/UE se modifica como sigue:

1) El artículo 10 se modifica como sigue:

a) en el apartado 7, la letra c) se sustituye por el texto siguiente:

«c) una demostración de cómo las funciones esenciales y las ramas de actividad principales podrían separarse jurídica y económicamente de otras funciones, en la medida en que sea necesario, para asegurar la continuidad y la resiliencia operativa digital en caso de inviabilidad de la entidad;»;

b) en el apartado 7, la letra q) se sustituye por el texto siguiente:

«q) una descripción de las operaciones y sistemas esenciales para mantener el funcionamiento continuado de los procesos operativos de la entidad, con inclusión de las redes y sistemas de información a que se refiere el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*);

(*) 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 (DO L 333 de 27.12.2022, p. 1).»;

c) en el apartado 9 se añade el párrafo siguiente:

«La ABE, de conformidad con lo dispuesto en el artículo 10 del Reglamento (UE) n.º 1093/2010, examinará las normas técnicas de regulación y, si procede, las actualizará a fin de tener en cuenta, entre otros aspectos, las disposiciones del capítulo II del Reglamento (UE) 2022/2554.».

2) El anexo se modifica como sigue:

a) en la sección A, el punto 16 se sustituye por el texto siguiente:

«16) disposiciones y medidas necesarias para mantener el funcionamiento continuado de los procesos operativos de la entidad, incluyendo las redes y los sistemas de información que se hayan establecido y gestionado de conformidad con el Reglamento (UE) 2022/2554;»;

b) la sección B queda modificada como sigue:

i) el punto 14 se sustituye por el texto siguiente:

«14) la identificación de los propietarios de los sistemas a que se hace referencia en el punto 13, de los acuerdos de nivel de servicio relacionados y de cualquier sistema informático o licencia, incluida la asignación a las personas jurídicas, las operaciones esenciales y las ramas de actividad principales de la entidad, así como la identificación de proveedores terceros esenciales de servicios de TIC, tal como se define en el artículo 3, punto 23, del Reglamento (UE) 2022/2554;»,

ii) se inserta el punto siguiente:

«14 bis) los resultados de las pruebas de resiliencia operativa digital de las entidades con arreglo al Reglamento (UE) 2022/2554;»;

c) la sección C queda modificada como sigue:

i) el punto 4 se sustituye por el texto siguiente:

«4) el grado en que los acuerdos de servicio que la entidad mantiene, incluidos acuerdos contractuales sobre el uso de servicios de TIC, son sólidos y plenamente ejecutables en caso de resolución de la entidad;»,

ii) se inserta el punto siguiente:

«4 bis) La resiliencia operativa digital de las redes y los sistemas de información que respaldan las funciones esenciales y las ramas de actividad principales de la entidad, teniendo en cuenta los informes de incidentes graves relacionados con las TIC y los resultados de las pruebas de resiliencia operativa digital con arreglo al Reglamento (UE) 2022/2554;».

Artículo 6

Modificaciones de la Directiva 2014/65/UE

La Directiva 2014/65/UE se modifica como sigue:

1) El artículo 16 se modifica como sigue:

a) el apartado 4 se sustituye por el texto siguiente:

«4. Toda empresa de servicios de inversión adoptará medidas razonables para garantizar la continuidad y la regularidad de la realización de los servicios y actividades de inversión. A tal fin, la empresa de servicios de inversión empleará sistemas adecuados y proporcionados, incluidos sistemas de tecnología de la información y la comunicación (TIC) establecidos y gestionados de conformidad con el artículo 7 del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), así como recursos y procedimientos adecuados y proporcionados.

(*) 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 (DO L 333 de 27.12.2022, p. 1).»;

b) en el apartado 5, los párrafos segundo y tercero se sustituyen por el texto siguiente:

«Toda empresa de servicios de inversión dispondrá de procedimientos administrativos y contables adecuados, mecanismos de control interno y técnicas eficaces de valoración del riesgo.

Sin perjuicio de la facultad de las autoridades competentes para exigir acceso a las comunicaciones de conformidad con lo dispuesto en la presente Directiva y en el Reglamento (UE) n.º 600/2014, la empresa de servicios de inversión deberá contar con mecanismos de seguridad sólidos para garantizar, de conformidad con los requisitos establecidos en el Reglamento (UE) 2022/2554, la seguridad y autenticación de los medios de transmisión de la información, para reducir al mínimo el riesgo de corrupción de datos y de acceso no autorizado, y evitar fugas de información, manteniendo en todo momento la confidencialidad de los datos.».

2) El artículo 17 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. La empresa de servicios de inversión que se dedique a la negociación algorítmica deberá implantar sistemas y controles de riesgo adecuados a sus actividades y eficaces para garantizar que sus sistemas de negociación sean resistentes y tengan suficiente capacidad de conformidad con los requisitos establecidos en el capítulo II del Reglamento (UE) 2022/2554, se ajusten a los umbrales y límites de negociación apropiados, y limiten o impidan el envío de órdenes erróneas o la posibilidad de que los sistemas funcionen de modo que pueda crear o propiciar anomalías en las condiciones de negociación.

Tal empresa deberá además implantar sistemas y controles de riesgo eficaces para garantizar que los sistemas de negociación no puedan usarse con ningún fin contrario al Reglamento (UE) n.º 596/2014 o a las normas del centro de negociación al que está vinculada.

Deberá implantar unos mecanismos eficaces que garanticen la continuidad de las actividades en caso de disfunción de sus sistemas de negociación, que incluyan políticas y planes de continuidad de las actividades de TIC y planes de respuesta y recuperación en materia de TIC establecidos de conformidad con el artículo 11 del Reglamento (UE) 2022/2554, y se asegurará de que sus sistemas sean íntegramente probados y convenientemente supervisados para garantizar que cumplen los requisitos generales establecidos en el presente apartado y cualesquiera requisitos específicos establecidos en los capítulos II y IV del Reglamento (UE) 2022/2554.»;

b) en el apartado 7, la letra a) se sustituye por el texto siguiente:

«a) los detalles de los requisitos de organización a que se refieren los apartados 1 a 6, salvo los relacionados con la gestión de riesgos relacionados con las TIC, que se exigirán a las empresas de servicios de inversión que presten distintos servicios de inversión, actividades de inversión, servicios auxiliares o combinaciones de los mismos, estableciendo las indicaciones relativas a los requisitos de organización estipulados en el apartado 5 de tal modo los requisitos específicos para el acceso directo al mercado y para el acceso patrocinado que se garantice que los controles aplicados al acceso patrocinado sean como mínimo equivalentes a los aplicados al acceso directo;».

3) En el artículo 47, el apartado 1 se modifica como sigue:

a) la letra b) se sustituye por el texto siguiente:

«b) esté adecuadamente equipado para gestionar los riesgos a los que está expuesto, incluida la gestión del riesgo relacionado con las TIC de conformidad con el capítulo II del Reglamento (UE) 2022/2554, aplicar mecanismos y sistemas que le permitan detectar los riesgos significativos que comprometan su funcionamiento y establecer medidas eficaces para atenuar esos riesgos;»;

b) se suprime la letra c).

4) El artículo 48 se modifica como sigue:

a) el apartado 1 se sustituye por el texto siguiente:

«1. Los Estados miembros exigirán que los mercados regulados establezcan y mantengan su resiliencia operativa de conformidad con los requisitos establecidos en el capítulo II del Reglamento (UE) 2022/2554, a fin de garantizar que sus sistemas de negociación sean resistentes, tengan capacidad suficiente para tramitar los volúmenes de órdenes y mensajes correspondientes a los momentos de máxima actividad, puedan asegurar la negociación ordenada en condiciones de fuerte tensión del mercado, se hayan probado íntegramente para garantizar el cumplimiento de esas condiciones y estén sujetos a mecanismos eficaces de continuidad de la actividad, con inclusión de políticas y planes de continuidad de las actividades de las TIC y planes de respuesta y recuperación en materia de TIC establecidos de conformidad con lo dispuesto en el artículo 11 del Reglamento (UE) 2022/2554, para asegurar el mantenimiento de sus servicios en caso de disfunción de sus sistemas de negociación.»;

b) el apartado 6 se sustituye por el texto siguiente:

«6. Los Estados miembros exigirán que los mercados regulados implanten sistemas, procedimientos y mecanismos eficaces, que también exijan a los miembros o participantes que realicen pruebas adecuadas de algoritmos y proporcionen los entornos que faciliten dichas pruebas de conformidad con los requisitos establecidos en los capítulos II y IV del Reglamento (UE) 2022/2554, para garantizar que los sistemas de negociación algorítmica no puedan generar anomalías en las condiciones de negociación en el mercado, ni contribuir a tales anomalías, y gestionar anomalías en las condiciones de negociación que puedan surgir de tales sistemas de negociación algorítmica, incluidos sistemas que permitan limitar la proporción de órdenes de operaciones no ejecutadas que un miembro o participante podrá introducir en el sistema, ralentizar el flujo de órdenes ante el riesgo de que se alcance el límite de capacidad del sistema y restringir el valor mínimo de variación del precio que podrá ejecutarse en el mercado, así como velar por su respeto.»;

c) el apartado 12 se modifica como sigue:

i) la letra a) se sustituye por el texto siguiente:

«a) los requisitos que garanticen que los sistemas de negociación de los mercados regulados sean resistentes y tengan una capacidad adecuada, salvo los requisitos relacionados con la resiliencia operativa digital;»,

ii) la letra g) se sustituye por el texto siguiente:

«g) los requisitos que garanticen que haya pruebas adecuadas de algoritmos, distintas de las pruebas de resiliencia operativa digital, a fin de asegurarse de que los sistemas de negociación algorítmica, incluidos los de alta frecuencia, no puedan ocasionar anomalías en las condiciones de negociación en el mercado, ni contribuir a tales anomalías.».

Artículo 7

Modificaciones de la Directiva (UE) 2015/2366

La Directiva (UE) 2015/2366 se modifica como sigue:

1) En el artículo 3, la letra j) se sustituye por el texto siguiente:

«j) los servicios prestados por proveedores de servicios técnicos como soporte a la prestación de servicios de pago, sin que dichos proveedores lleguen a estar en ningún momento en posesión de los fondos que deban transferirse, incluidos el tratamiento y almacenamiento de datos, los servicios de confianza y de protección de la intimidad, la autenticación de datos y entidades, el suministro de tecnología de la información y la comunicación (TIC) y redes de comunicación, y el suministro y mantenimiento de terminales y dispositivos empleados para los servicios de pago, con exclusión de los servicios de iniciación de pagos y servicios de información sobre cuentas;».

2) En el artículo 5, el apartado 1 se modifica como sigue:

a) el párrafo primero se modifica como sigue:

i) la letra e) se sustituye por el texto siguiente:

«e) una descripción de los métodos de gobierno empresarial y de los mecanismos de control interno del solicitante, incluidos procedimientos administrativos, de gestión del riesgo y contables, así como de los mecanismos para la utilización de los servicios de TIC de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), que demuestre que dichos métodos de gobierno empresarial y mecanismos de control interno son proporcionados, apropiados, sólidos y adecuados;

(*) 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 (DO L 333 de 27.12.2022, p. 1).»,

ii) la letra f) se sustituye por el texto siguiente:

«f) una descripción del procedimiento establecido para la supervisión, la tramitación y el seguimiento de los incidentes de seguridad y las reclamaciones de los consumidores al respecto, incluido un mecanismo de notificación de incidentes que atienda a las obligaciones de notificación de la entidad de pago establecidas en el capítulo III del Reglamento (UE) 2022/2554;»,

iii) la letra h) se sustituye por el texto siguiente:

«h) una descripción de los mecanismos que garanticen la continuidad de la actividad, con inclusión de una delimitación clara de las operaciones esenciales, planes y política de continuidad de las actividades de TIC y planes de respuesta y recuperación en materia de TIC efectivos, así como un procedimiento para poner a prueba y revisar periódicamente la adecuación y eficiencia de dichos planes de conformidad con el Reglamento (UE) 2022/2554;»;

b) el párrafo tercero se sustituye por el texto siguiente:

«Las medidas de control de la seguridad y mitigación de los riesgos a que se refiere la letra j) del párrafo primero deberán indicar de qué manera garantizan un elevado nivel de resiliencia operativa digital de conformidad con el capítulo II del Reglamento (UE) 2022/2554, en particular en relación con la seguridad técnica y la protección de datos, también en lo que respecta a los soportes lógicos y los sistemas de TIC utilizados por el solicitante o por las empresas a las que externalice la totalidad o parte de sus operaciones. Dichas medidas comprenderán asimismo las medidas de seguridad establecidas en el artículo 95, apartado 1, de la presente Directiva, y atenderán a las directrices sobre medidas de seguridad formuladas por la ABE a que se refiere el artículo 95, apartado 3, de la presente Directiva cuando se adopten.».

3) En el artículo 19, apartado 6, el párrafo segundo se sustituye por el texto siguiente:

«La externalización de funciones operativas importantes, incluidos los sistemas de TIC, deberá realizarse de modo tal que no afecte significativamente ni a la calidad del control interno de la entidad de pago ni a la capacidad de las autoridades competentes para controlar y hacer un seguimiento *a posteriori* del cumplimiento por la entidad de pago de todas las obligaciones que establece la presente Directiva.».

4) En el artículo 95, apartado 1, se añade el párrafo siguiente:

«El párrafo primero se entenderá sin perjuicio de la aplicación del capítulo II del Reglamento (UE) 2022/2554 a:

a) los proveedores de servicios de pago a que se refiere el artículo 1, apartado 1, letras a), b) y d), de la presente Directiva;

b) los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la presente Directiva;

c) las entidades de pago exentas en virtud del artículo 32, apartado 1, de la presente Directiva, y

d) las entidades de dinero electrónico que se benefician de una excepción a que se refiere el artículo 9, apartado 1, de la Directiva 2009/110/CE.».

5) En el artículo 96 se añade el apartado siguiente:

«7. Los Estados miembros garantizarán que los apartados 1 a 5 del presente artículo no se apliquen a:

a) los proveedores de servicios de pago a que se refiere el artículo 1, apartado 1, letras a), b) y d), de la presente Directiva;

b) los proveedores de servicios de información sobre cuentas a que se refiere el artículo 33, apartado 1, de la presente Directiva;

c) las entidades de pago exentas en virtud del artículo 32, apartado 1, de la presente Directiva, y

d) las entidades de dinero electrónico que se benefician de una excepción a que se refiere el artículo 9, apartado 1, de la Directiva 2009/110/CE.».

6) En el artículo 98, el apartado 5 se sustituye por el texto siguiente:

«5. La ABE, de conformidad con lo dispuesto en el artículo 10 del Reglamento (UE) n.º 1093/2010, examinará periódicamente las normas técnicas de regulación y, si ha lugar, las actualizará a fin de tener en cuenta, entre otros aspectos, las innovaciones y la evolución tecnológica, así como las disposiciones del capítulo II del Reglamento (UE) 2022/2554.».

Artículo 8

Modificaciones de la Directiva (UE) 2016/2341

En el artículo 21 de la Directiva (UE) 2016/2341, el apartado 5 se sustituye por el texto siguiente:

«5. Los Estados miembros velarán por que los FPE adopten medidas razonables para garantizar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de emergencia. A tal fin, los FPE

emplearán sistemas, recursos y procedimientos adecuados y proporcionados y en particular implantarán y gestionarán redes y sistemas de información de conformidad con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo (*), cuando proceda.

(*) Reglamento (UE) 2022/2554del 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 (DO L 333 de 27.12.2022, p. 1).».

Artículo 9

Transposición

1. Los Estados miembros adoptarán y publicarán a más tardar el 17 de enero de 2025, las disposiciones necesarias para dar cumplimiento a lo dispuesto en la presente Directiva. Informarán inmediatamente de ello a la Comisión.

Aplicarán dichas disposiciones a partir del 17 de enero de 2025.

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

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

Artículo 10

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 11

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

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 2008/114/CE del Consejo

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

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

Visto el dictamen del Comité de las Regiones ([2]),

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

Considerando lo siguiente:

(1) Por su condición de proveedoras de servicios esenciales, las entidades críticas son indispensables para mantener las funciones sociales o las actividades económicas vitales en el mercado interior, con una economía de la Unión cada vez más interdependiente. Por ello es esencial establecer un marco de la Unión con el fin de aumentar la resiliencia de las entidades críticas en el mercado interior fijando unas normas mínimas armonizadas, y de prestarles asistencia mediante un apoyo coherente y específico y medidas de supervisión.

(2) La Directiva 2008/114/CE del Consejo ([4]) establece un procedimiento para designar las infraestructuras críticas europeas en los sectores de la energía y el transporte cuya perturbación o destrucción tendría repercusiones transfronterizas significativas en al menos dos Estados miembros. Dicha Directiva se centra exclusivamente en la protección de tales infraestructuras. Sin embargo, la evaluación de la Directiva 2008/114/CE realizada en 2019 puso de manifiesto que, debido al carácter cada vez más interconectado y transfronterizo de las operaciones que utilizan infraestructuras críticas, las medidas de protección relativas únicamente a activos individuales no bastan para evitar que se produzcan todas las perturbaciones. Por lo tanto, es necesario modificar el enfoque para garantizar que se tengan mejor en cuenta los riesgos, se mejore la definición y la coherencia de la función y las obligaciones de las entidades críticas que prestan servicios esenciales para el funcionamiento del mercado interior, y

([1]) DO C 286 de 16.7.2021, p. 170.
([2]) DO C 440 de 29.10.2021, p. 99.
([3]) Posición del Parlamento Europeo de 22 de noviembre de 2022 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 8 de diciembre de 2022.
([4]) Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

se adopten normas de la Unión a fin de aumentar la resiliencia de las entidades críticas. Las entidades críticas han de poder reforzar su capacidad de prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación ante incidentes que puedan perturbar la prestación de servicios esenciales.

(3) Pese a que existen diversas medidas a escala de la Unión, como el Programa Europeo de Protección de Infraestructuras Vitales, y a escala nacional destinadas a apoyar la protección de las infraestructuras críticas en la Unión, las entidades que explotan tales infraestructuras han de estar mejor equipadas para hacer frente a los riesgos para sus operaciones que puedan dar lugar a una perturbación en la prestación de servicios esenciales. También se debe hacer más por equipar mejor a tales entidades dada la existencia de un panorama dinámico de amenazas, entre las que figuran las amenazas híbridas y terroristas en evolución y las crecientes interdependencias entre infraestructura y sectores. Además, ha aumentado el riesgo físico derivado de las catástrofes naturales y del cambio climático, que intensifica la frecuencia y la magnitud de los fenómenos meteorológicos extremos e introduce cambios a largo plazo en las condiciones climáticas medias que pueden mermar la capacidad, la eficiencia y la vida útil de determinados tipos de infraestructuras si no existen medidas de adaptación al cambio climático. Además, el mercado interior se caracteriza por la fragmentación en lo que respecta a la identificación de las entidades críticas, pues los sectores y categorías de entidades pertinentes no se reconocen sistemáticamente como críticos en todos los Estados miembros. Por consiguiente, la presente Directiva debe lograr un nivel sustancial de armonización en lo que se refiere a los sectores y categorías de entidades que entran en su ámbito de aplicación.

(4) Si bien determinados sectores de la economía, como los sectores de la energía y del transporte, ya están regulados mediante actos jurídicos sectoriales de la Unión, dichos actos jurídicos contienen disposiciones relativas únicamente a determinados aspectos de la resiliencia de las entidades que operan en dichos sectores. Con el fin de abordar de manera global la resiliencia de las entidades que son vitales para el correcto funcionamiento del mercado interior, la presente Directiva crea un marco general que aborda la resiliencia de las entidades críticas con respecto a todos los peligros, ya sean naturales, o provocados, accidental o intencionadamente, por el ser humano.

(5) Las crecientes interdependencias entre infraestructuras y sectores son el resultado de una red cada vez más transfronteriza e interdependiente de prestación de servicios que utiliza infraestructuras clave en toda la Unión en los sectores de la energía, el transporte, la banca, el agua potable, las aguas residuales, la producción, transformación y distribución de productos alimentarios, la sanidad, el espacio, la infraestructura de los mercados financieros y la infraestructura digital, y en ciertos aspectos del sector de la Administración pública. El sector espacial se inscribe en el ámbito de aplicación de la presente Directiva en lo que respecta a la prestación de determinados servicios que dependen de infraestructuras terrestres cuya propiedad, gestión y explotación corresponde a Estados miembros o a entidades privadas; por consiguiente, las infraestructuras cuya propiedad, gestión y explotación corresponde a la Unión o se efectúa en su nombre como parte de su programa espacial no entran en el ámbito de la presente Directiva.

Por lo que se refiere al sector energético y, en particular, a los métodos de generación y transporte de electricidad (en relación con el suministro de electricidad), se sobreentiende que, toda vez que se estime oportuno, pueden incluirse en la generación de energía eléctrica los elementos de transmisión eléctrica de las centrales nucleares, pero se excluyen los elementos específicamente nucleares regulados por tratados y por el Derecho de la Unión, incluidos los actos jurídicos pertinentes de la Unión relativos a la energía nuclear. El proceso de identificación de las entidades críticas en el sector alimentario debe reflejar adecuadamente la naturaleza del mercado interior en dicho sector y las amplias normas de la Unión relativas a los principios y requisitos generales de la legislación y la seguridad alimentarias. Por consiguiente, a fin de garantizar una estrategia proporcionada y de reflejar adecuadamente el papel y la importancia de dichas entidades a escala nacional, las entidades críticas únicamente deben incluir las empresas alimentarias, ya sean públicas o privadas, con o sin ánimo de lucro, que se dediquen exclusivamente a la logística y distribución al por mayor y la producción y transformación industrial a gran escala que registren una cuota de mercado importante a escala nacional. Dichas interdependencias suponen que cualquier perturbación de los servicios esenciales, incluso inicialmente limitada a una entidad o a un sector, puede producir efectos en cascada más amplios, lo que podría tener una repercusión negativa de gran alcance y duradera para la prestación de servicios en todo el mercado interior. Las grandes crisis, como la pandemia de COVID-19, han puesto de manifiesto la vulnerabilidad de nuestras sociedades, cada vez más interdependientes, frente a riesgos de baja probabilidad que tengan grandes repercusiones.

(6) Las entidades que intervienen en la prestación de servicios esenciales están cada vez más sujetas a requisitos divergentes impuestos por el Derecho nacional. El hecho de que algunos Estados miembros tengan unos requisitos menos estrictos para esas entidades no solo conduce a distintos niveles de resiliencia, sino que también puede afectar negativamente al mantenimiento de funciones sociales o actividades económicas vitales en toda la Unión y obstaculiza el correcto funcionamiento del mercado interior. Los inversores y las empresas pueden confiar en las entidades críticas que sean resilientes y fiarse de ellas, al ser la confianza y la fiabilidad las piedras angulares de un mercado interior que funciona correctamente. Los tipos de entidades similares se consideran críticos en algunos Estados miembros pero no en otros, y las entidades consideradas críticas están sujetas a requisitos divergentes en distintos Estados miembros. Ello da lugar a una carga administrativa adicional e innecesaria para las empresas que realizan operaciones transfronterizas, en particular en el caso de aquellas que tienen actividad en Estados miembros con unos requisitos más estrictos. Por consiguiente, un marco de la Unión también implicaría unas condiciones de competencia equitativas para las entidades críticas en toda la Unión.

(7) Es necesario establecer unas normas mínimas armonizadas para garantizar la prestación de servicios esenciales en el mercado interior, aumentar la resiliencia de las entidades críticas y mejorar la cooperación transfronteriza entre las autoridades competentes. Es importante que la concepción y la aplicación de estas normas estén preparadas para el futuro, al mismo tiempo que se permite la flexibilidad necesaria. También es crucial mejorar la capacidad de las entidades críticas para prestar servicios esenciales frente a distintos riesgos.

(8) A fin de alcanzar un alto grado de resiliencia, los Estados miembros deben identificar las entidades críticas que van a estar sujetas a unos requisitos y una supervisión específicos y a las que se va a brindar apoyo y orientación específicos frente a todos los riesgos pertinentes.

(9) Dada la importancia de la ciberseguridad para la resiliencia de las entidades críticas y en aras de la coherencia, debe garantizarse, siempre que sea posible, un enfoque coherente entre la presente Directiva y la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([5]). Teniendo en cuenta la mayor frecuencia y las características particulares de los riesgos cibernéticos, la Directiva (UE) 2022/2555 impone unos requisitos exhaustivos a un amplio conjunto de entidades para garantizar su ciberseguridad. Dado que la ciberseguridad se trata de manera suficiente en la Directiva (UE) 2022/2555, las materias reguladas por dicha Directiva deben quedar excluidas del ámbito de aplicación de la presente Directiva, sin perjuicio del régimen particular aplicable a las entidades del sector de las infraestructuras digitales.

(10) A fin de evitar duplicidades y cargas innecesarias, las disposiciones pertinentes de la presente Directiva no deben aplicarse si las disposiciones de actos jurídicos sectoriales de la Unión obligan a las entidades críticas a adoptar medidas para aumentar su resiliencia y tales obligaciones son reconocidas por los Estados miembros como al menos equivalentes a las obligaciones correspondientes establecidas en la presente Directiva. En tal caso, deben aplicarse las disposiciones pertinentes de esos otros actos jurídicos de la Unión. Cuando no sean de aplicación las disposiciones pertinentes de la presente Directiva, las disposiciones en materia de supervisión y ejecución establecidas en ella tampoco deben aplicarse.

(11) La presente Directiva no afecta a las competencias de los Estados miembros y sus autoridades por lo que respecta a la autonomía administrativa ni a su responsabilidad de preservar la seguridad nacional y la defensa o de sus competencias de salvaguardar otras funcionales esenciales del Estado, en particular por lo que atañe a la seguridad pública, la integridad territorial y el mantenimiento del orden público. La exclusión de las entidades de la administración pública del ámbito de aplicación de la presente Directiva debe aplicarse a las entidades que realicen sus actividades predominantemente en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación de la ley, con inclusión de la investigación, la detección y el enjuiciamiento de infracciones penales. No obstante, las entidades de la administración pública cuyas actividades estén mínimamente relacionadas con dichos ámbitos deben entrar en el 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 aplicación de la ley y, por lo tanto, no quedan excluidas por ese motivo de su ámbito de aplicación. Las entidades de la administración pública establecidas conjuntamente con un tercer país de conformidad con un acuerdo internacional no entran en el 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.

([5]) 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 se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (véase la página 80 del presente Diario Oficial).

Determinadas entidades críticas realizan actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación de la ley, con inclusión de la investigación, la detección y el enjuiciamiento de infracciones penales, o prestan servicios exclusivamente a entidades de la administración pública que realizan actividades predominantemente en dichos ámbitos. Habida cuenta de la responsabilidad de los Estados miembros de salvaguardar la seguridad nacional y la defensa, los Estados miembros deben poder decidir que las obligaciones de las entidades críticas establecidas en la presente Directiva no se apliquen total o parcialmente a dichas entidades críticas si los servicios que prestan o las actividades que realizan están relacionadas predominantemente con los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación de la ley, con inclusión de la investigación, la detección y el enjuiciamiento de infracciones penales. Las entidades críticas cuyos servicios o actividades solo estén mínimamente relacionados con dichos ámbitos deben seguir en el ámbito de aplicación de la presente Directiva. No se debe obligar a ningún Estado miembro a facilitar información cuya divulgación sea contraria a los intereses esenciales de su seguridad nacional. Son pertinentes las normas de la Unión o nacionales en materia de protección de la información clasificada, y los acuerdos de confidencialidad.

(12) Para no poner en peligro la seguridad nacional ni la seguridad y los intereses comerciales de las entidades críticas, el acceso a información delicada así como su intercambio y tratamiento deben efectuarse con prudencia, prestando especial atención a los canales de transmisión y las capacidades de almacenamiento que se utilicen.

(13) Con el fin de garantizar un enfoque global de la resiliencia de las entidades críticas, cada Estado miembro debe contar con una estrategia que mejore la resiliencia de las entidades críticas (en lo sucesivo, «estrategia»). La estrategia debe establecer los objetivos estratégicos y las medidas de actuación que hayan de aplicarse. En aras de la coherencia y la eficiencia, la estrategia debe estar diseñada para integrarse adecuadamente en las políticas vigentes, a partir, siempre que sea posible, de estrategias nacionales y sectoriales, planes o documentos similares existentes en la materia. A fin de alcanzar un enfoque global, los Estados miembros deben garantizar que sus estrategias establezcan un marco de actuación para mejorar la coordinación entre las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555, en el contexto del intercambio de información sobre los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella y en el contexto del ejercicio de las tareas de supervisión. Al poner en marcha sus estrategias, los Estados miembros deben tener debidamente en cuenta la naturaleza híbrida de las amenazas para las entidades críticas.

(14) Los Estados miembros deben comunicar a la Comisión sus estrategias y las actualizaciones sustanciales de estas, en particular para que la Comisión pueda evaluar la correcta aplicación de la presente Directiva en lo que se refiere a los enfoques estratégicos sobre la resiliencia de las entidades críticas a escala nacional. En caso necesario, las estrategias podrían comunicarse como información clasificada. La Comisión debe elaborar un informe de síntesis de las estrategias comunicadas por los Estados miembros que sirva de base para los intercambios a fin de determinar las mejores prácticas y las cuestiones de interés común en el marco de un Grupo de Resiliencia de las Entidades Críticas. Debido al carácter delicado de la información incluida en el informe de síntesis, clasificada o no, la Comisión debe tratar el informe de síntesis con el nivel pertinente de concienciación en lo que respecta a la seguridad de las entidades críticas, los Estados miembros y la Unión. El informe de síntesis y las estrategias deben protegerse contra acciones ilícitas o malintencionadas y únicamente deben ser accesibles para las personas autorizadas con el fin de alcanzar los objetivos de la presente Directiva. La comunicación de las estrategias y las actualizaciones sustanciales de estas también deben ayudar a la Comisión a comprender la evolución de los enfoques de resiliencia de las entidades críticas y contribuir al seguimiento del impacto y el valor añadido de la presente Directiva, que la Comisión debe revisar periódicamente.

(15) Las acciones de los Estados miembros para identificar las entidades críticas y ayudarlas a asegurar su resiliencia deben seguir un enfoque basado en el riesgo que se centre en las entidades más pertinentes para el desempeño de funciones sociales o actividades económicas vitales. A fin de garantizar este enfoque específico, cada Estado miembro debe realizar, en un marco armonizado, una evaluación de los riesgos naturales y de origen humano pertinentes, incluidos los de carácter transfronterizo o intersectorial, que puedan afectar a la prestación de servicios esenciales, incluidos los accidentes, las catástrofes naturales, las emergencias de salud pública como las pandemias y las amenazas híbridas u otras amenazas antagónicas, incluidos los delitos de terrorismo, la infiltración delictiva y el sabotaje (en lo sucesivo, «evaluación de riesgos del Estado miembro»). Al realizar las evaluaciones de riesgos del Estado miembro, los Estados miembros deben tener en cuenta otras evaluaciones de riesgos generales o sectoriales que se hayan realizado en virtud de otros actos jurídicos de la Unión y deben considerar hasta qué punto unos sectores dependen de otros, incluidos los sectores de otros Estados miembros y de terceros países. Los resultados de las evaluaciones de riesgos del Estado miembro deben utilizarse a fin de identificar las entidades críticas y de

ayudarlas a cumplir sus requisitos de resiliencia. La presente Directiva se aplica únicamente a los Estados miembros y a las entidades críticas que actúan dentro de la Unión. No obstante, la experiencia y los conocimientos generados por las autoridades competentes, en particular mediante las evaluaciones de riesgos, así como por la Comisión, en particular a través de diversas formas de apoyo y cooperación, podrían utilizarse, cuando proceda y de conformidad con los instrumentos jurídicos aplicables, en beneficio de terceros países, en particular los de la vecindad directa de la Unión, al contribuir a la cooperación existente en materia de resiliencia.

(16) A fin de garantizar que todas las entidades pertinentes estén sujetas a los requisitos de resiliencia de la presente Directiva y reducir las divergencias a ese respecto, es importante establecer normas armonizadas que posibiliten una identificación coherente de las entidades críticas en toda la Unión, permitiendo al mismo tiempo que los Estados miembros reflejen adecuadamente la función y la importancia de dichas entidades a escala nacional. Al aplicar los criterios establecidos en la presente Directiva, cada Estado miembro debe identificar las entidades que presten uno o varios servicios esenciales y que operen en su territorio y tengan infraestructuras críticas situadas en él. Debe considerarse que una entidad opera en el territorio de un Estado miembro en el que realice actividades necesarias para el servicio o servicios esenciales en cuestión, y en el que se sitúe la infraestructura crítica de dicha entidad que se utilice para prestar ese servicio o servicios. Cuando en algún Estado miembro no exista ninguna entidad que cumpla dichos criterios, dicho Estado miembro no debe estar obligado a identificar una entidad crítica en el sector o subsector correspondiente. En aras de la eficacia, la eficiencia, la coherencia y la seguridad jurídica, deben establecerse normas adecuadas en lo que respecta a la notificación a las entidades de que han sido identificadas como entidades críticas.

(17) Los Estados miembros deben presentar a la Comisión, de tal manera que se cumplan los objetivos de la presente Directiva, una lista de los servicios esenciales, el número de entidades críticas identificadas en relación con cada uno de los sectores y subsectores indicados en el anexo y en relación con el servicio o los servicios esenciales que preste cada entidad y, si se aplican, los umbrales. Debe ser posible presentar umbrales como tales o en forma agregada, de forma que se pueda calcular una media de los datos por zona geográfica, año, sector, subsector u otros criterios, y entre los que puede figurar información sobre el conjunto de indicadores facilitados.

(18) Deben establecerse criterios para determinar el carácter significativo de un efecto perturbador producido por un incidente. Esos criterios deben basarse en los establecidos en la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([6]), a fin de aprovechar los esfuerzos realizados por los Estados miembros para identificar los operadores de servicios esenciales tal como se definen en dicha Directiva y la experiencia adquirida a ese respecto. Las grandes crisis, como la pandemia de COVID-19, han puesto de manifiesto la importancia de garantizar la seguridad de la cadena de suministro y han demostrado cómo su perturbación puede tener repercusiones económicas y sociales negativas en un gran número de sectores y a través de las fronteras. Por consiguiente, los Estados miembros también deben tener en cuenta, en la medida de lo posible, los efectos en la cadena de suministro al determinar hasta qué punto otros sectores y subsectores dependen del servicio esencial prestado por una entidad crítica.

(19) De conformidad con el Derecho de la Unión y nacional aplicable, incluido el Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo ([7]), que establece un marco para el control de las inversiones extranjeras directas en la Unión, debe reconocerse la amenaza potencial que plantea la propiedad extranjera de infraestructuras críticas dentro de la Unión, ya que los servicios, la economía y la libre circulación y seguridad de los ciudadanos de la Unión dependen del correcto funcionamiento de las infraestructuras críticas.

(20) La Directiva (UE) 2022/2555 obliga a las entidades pertenecientes al sector de las infraestructuras digitales, las cuales podrían ser identificadas como entidades críticas con arreglo a la presente Directiva, a adoptar las medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos de seguridad de los sistemas de redes y de información, así como a notificar los incidentes significativos y ciberamenazas. Puesto que las amenazas a la seguridad de los sistemas de redes y de información pueden tener diferentes orígenes, la Directiva (UE) 2022/2555 aplica un enfoque de «todos los riesgos posibles» que incluye la resiliencia de los sistemas de redes y de información, así como los componentes físicos y el entorno de dichos sistemas.

([6]) 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).

([7]) Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión (DO L 79 I de 21.3.2019, p. 1).

Dado que los requisitos establecidos en la Directiva (UE) 2022/2555 a ese respecto son al menos equivalentes a las correspondientes obligaciones establecidas en la presente Directiva, las obligaciones establecidas en el artículo 11 y los capítulos III, IV y VI de la presente Directiva no deben aplicarse a las entidades pertenecientes al sector de las infraestructuras digitales, a fin de evitar duplicidades y cargas administrativas innecesarias. No obstante, teniendo en cuenta la importancia de los servicios prestados por las entidades pertenecientes al sector de las infraestructuras digitales para las entidades críticas pertenecientes a todos los demás sectores, los Estados miembros deben identificar, sobre la base de los criterios y utilizando el procedimiento previsto en la presente Directiva, como entidades críticas a las entidades pertenecientes al sector de las infraestructuras digitales. Deben, por consiguiente, aplicarse las estrategias, las evaluaciones de riesgos del Estado miembro y las medidas de apoyo establecidas en el capítulo II de la presente Directiva. Los Estados miembros deben poder adoptar o mantener disposiciones de Derecho nacional destinadas a alcanzar un mayor nivel de resiliencia de dichas entidades críticas, a condición de que dichas disposiciones sean coherentes con el Derecho de la Unión aplicable.

(21) El Derecho de la Unión en materia de servicios financieros establece requisitos exhaustivos para que las entidades financieras gestionen todos los riesgos a los que se enfrentan, incluidos los riesgos operativos, y garanticen la continuidad de las actividades. Este Derecho incluye los Reglamentos (UE) n.º 648/2012 ([8]), (UE) n.º 575/2013 ([9]) y (UE) n.º 600/2014 ([10]) del Parlamento Europeo y del Consejo y las Directivas 2013/36/UE ([11]) y 2014/65/UE ([12]) del Parlamento Europeo y del Consejo. Dicho marco jurídico se complementa con el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([13]), que establece los requisitos aplicables a las entidades financieras que gestionen riesgos relacionados con las tecnologías de la información y de las comunicaciones (TIC), incluidos los relativos a la protección de las infraestructuras físicas de las TIC. Dado que la resiliencia de dichas entidades está, por tanto, ampliamente cubierta, el artículo 11 y los capítulos III, IV y VI de la presente Directiva no deben aplicarse a dichas entidades, a fin de evitar duplicidades y cargas administrativas innecesarias.

No obstante, teniendo en cuenta la importancia de los servicios prestados por las entidades en el sector financiero a las entidades críticas pertenecientes a todos los demás sectores, los Estados miembros deben identificar, sobre la base de los criterios y utilizando el procedimiento previsto en la presente Directiva, a entidades del sector financiero como entidades críticas. Por consiguiente, se deben aplicar las estrategias, las evaluaciones de riesgos del Estado miembro y las medidas de apoyo establecidas en el capítulo II de la presente Directiva. Los Estados miembros deben poder adoptar o mantener disposiciones de Derecho nacional destinadas a alcanzar un mayor nivel de resiliencia de dichas entidades críticas, a condición de que dichas disposiciones sean coherentes con el Derecho de la Unión aplicable.

(22) Los Estados miembros deben designar o establecer autoridades competentes para supervisar la aplicación y, en su caso, hacer cumplir las normas de la presente Directiva, y garantizar que dichas autoridades dispongan de las competencias y los recursos adecuados. Habida cuenta de las diferencias existentes entre las estructuras de gobernanza nacionales, y con el fin de salvaguardar los acuerdos sectoriales o los organismos de supervisión y regulación de la Unión existentes y de evitar duplicidades, los Estados miembros deben poder designar o establecer más de una autoridad competente. Si designan o establecen más de una autoridad competente, los Estados miembros deben delimitar claramente las tareas respectivas de las autoridades interesadas y garantizar una cooperación fluida y eficaz. Todas las autoridades competentes también deben cooperar de manera más general con otras autoridades pertinentes, tanto a nivel de la Unión como nacional.

([8]) 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).

([9]) 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).

([10]) Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 173 de 12.6.2014, p. 84).

([11]) Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

([12]) 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).

([13]) 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).

(23) A fin de facilitar la cooperación y la comunicación transfronterizas y permitir la aplicación efectiva de la presente Directiva, cada Estado miembro debe designar, sin perjuicio de los requisitos de los actos jurídicos sectoriales de la Unión, un punto de contacto único encargado de coordinar las cuestiones relacionadas con la resiliencia de las entidades críticas y la cooperación transfronteriza a escala de la Unión (en lo sucesivo, «punto de contacto único»), dentro de una autoridad competente cuando proceda. Cada punto de contacto único debe servir de enlace y coordinar la comunicación, cuando proceda, con las autoridades competentes de su Estado miembro, con los puntos de contacto únicos de otros Estados miembros y con el Grupo de Resiliencia de las Entidades Críticas.

(24) Las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 deben cooperar e intercambiar información en relación con los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella que afecten a las entidades críticas, así como en relación con las medidas pertinentes adoptadas por las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555. Es importante que los Estados miembros garanticen que los requisitos establecidos en la presente Directiva y en la Directiva (UE) 2022/2555 se apliquen de forma complementaria y que las entidades críticas no estén sujetas a una carga administrativa superior a la necesaria para alcanzar los objetivos de la presente Directiva y de dicha Directiva.

(25) Los Estados miembros deben ayudar a las entidades críticas, también a las que tienen la condición de pequeñas y medianas empresas, a reforzar su resiliencia, de conformidad con las obligaciones de los Estados miembros establecidas en la presente Directiva, sin perjuicio de la responsabilidad jurídica propia de las entidades críticas de garantizar su cumplimiento y, de este modo, evitar las cargas administrativas excesivas. En particular, los Estados miembros podrían desarrollar materiales y metodologías de orientación, apoyar la organización de ejercicios para comprobar la resiliencia de las entidades críticas y proporcionar asesoramiento y formación al personal de las entidades críticas. Cuando sea necesario y esté justificado por objetivos de interés público, los Estados miembros pueden proporcionar recursos financieros y deben facilitar el intercambio voluntario de información y de buenas prácticas entre las entidades críticas, sin perjuicio de la aplicación de las normas de competencia establecidas en el Tratado de Funcionamiento de la Unión Europea (TFUE).

(26) Al objeto de aumentar la resiliencia de las entidades críticas identificadas por los Estados miembros y a fin de reducir las cargas administrativas de dichas entidades críticas, las autoridades competentes deben efectuar consultas entre sí, siempre que proceda, con el fin de garantizar que la presente Directiva se aplique de manera coherente. Dichas consultas deben celebrarse a instancia de cualquier autoridad competente interesada, y centrarse en garantizar un planteamiento convergente en lo relativo a las entidades críticas interconectadas que utilicen infraestructuras críticas físicamente conectadas entre dos o más Estados miembros, que pertenezcan a los mismos grupos o estructuras empresariales, o que se hayan identificado en un Estado miembro y que presten servicios esenciales a otros Estados miembros o en otros Estados miembros.

(27) Cuando el Derecho nacional o de la Unión disponga que las entidades críticas deben evaluar los riesgos pertinentes a efectos de la presente Directiva y tomar medidas para garantizar su propia resiliencia, tales requisitos deben tenerse debidamente en cuenta a los efectos de supervisar el cumplimiento por las entidades críticas de la presente Directiva.

(28) Las entidades críticas deben tener una comprensión cabal de los riesgos pertinentes a los que están expuestas y tener la obligación de analizar dichos riesgos. A tal fin, deben realizar evaluaciones de riesgos siempre que sea necesario, habida cuenta de sus circunstancias particulares y de la evolución de tales riesgos, y, en cualquier caso, cada cuatro años, para evaluar todos los riesgos pertinentes que puedan perturbar la prestación de sus servicios esenciales (en lo sucesivo, «evaluación de riesgos de la entidad crítica»). Cuando hayan realizado otras evaluaciones de riesgos o elaborado documentos en virtud de obligaciones establecidas en otros actos jurídicos que sean pertinentes para su evaluación de riesgos de la entidad crítica, las entidades críticas deben poder utilizar dichas evaluaciones y documentos para cumplir los requisitos establecidos en la presente Directiva en lo relativo a las evaluaciones de riesgos de la entidad crítica. Una autoridad competente debe poder declarar que una evaluación de riesgos existente realizada por una entidad crítica que aborde los riesgos y el grado de dependencia pertinentes cumple, total o parcialmente, con las obligaciones establecidas en la presente Directiva.

(29) Las entidades críticas deben adoptar medidas técnicas, organizativas, y de seguridad adecuadas y proporcionadas a los riesgos a los que se enfrenten a los efectos de prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación ante un incidente. Si bien las entidades críticas deben tomar dichas medidas de conformidad con la presente Directiva, los detalles y el alcance de tales medidas deben reflejar los diferentes riesgos que cada una de las entidades críticas haya determinado como parte de su evaluación de riesgos de la entidad crítica y las características específicas de dicha entidad de manera adecuada y proporcionada. A fin de promover un enfoque coherente a escala de la Unión, la Comisión, previa consulta al Grupo de Resiliencia de las Entidades Críticas, debe adoptar directrices no vinculantes para especificar con más detalle dichas medidas técnicas, organizativas y de seguridad. Los Estados miembros deben garantizar que cada entidad crítica designe a un agente de enlace o equivalente como punto de contacto con las autoridades competentes.

(30) En aras de la eficacia y la rendición de cuentas, las entidades críticas deben describir las medidas que adopten, con un nivel de detalle que permita alcanzar de manera suficiente los objetivos de eficacia y rendición de cuentas, teniendo en cuenta los riesgos detectados, en un plan de resiliencia, o en uno o varios documentos que sean equivalentes a un plan de resiliencia, y poner ese plan en práctica. La entidad crítica que ya haya adoptado medidas técnicas, organizativas y de seguridad y elaborado documentos en virtud de otros actos jurídicos que sean pertinentes para las medidas de aumento de la resiliencia en virtud de la presente Directiva, debe poder, a fin de evitar duplicidades, utilizar dichas medidas y documentos para cumplir los requisitos en materia de medidas de resiliencia con arreglo a la presente Directiva. A fin de evitar duplicidades, la autoridad competente debe poder declarar que las medidas de resiliencia existentes adoptadas por una entidad crítica que aborden sus obligaciones de adoptar medidas técnicas, organizativas y de seguridad con arreglo a la presente Directiva son conformes, total o parcialmente, con los requisitos de la presente Directiva.

(31) Los Reglamentos (CE) n.º 725/2004 ([14]) y (CE) n.º 300/2008 ([15]) del Parlamento Europeo y del Consejo y la Directiva 2005/65/CE del Parlamento Europeo y del Consejo ([16]) establecen requisitos aplicables a las entidades de los sectores del transporte aéreo y marítimo para prevenir incidentes causados por actos ilícitos, y para resistir y mitigar las consecuencias de tales incidentes. Si bien las medidas exigidas en virtud de la presente Directiva son más amplias en términos de riesgos y tipos de medidas que han de adoptarse, las entidades críticas de esos sectores deben reflejar en su plan de resiliencia o en los documentos equivalentes las medidas adoptadas en virtud de esos otros actos jurídicos de la Unión. Las entidades críticas también deben tener en cuenta la Directiva 2008/96/CE del Parlamento Europeo y del Consejo ([17]), que introduce una evaluación de las carreteras del conjunto de la red para cartografiar los riesgos de accidentes y una inspección específica de seguridad vial para detectar condiciones peligrosas, defectos y problemas que aumentan el riesgo de accidentes y lesiones, a partir de visitas *in situ* a carreteras o tramos de carreteras en servicio. Garantizar la protección y la resiliencia de las entidades críticas reviste la máxima importancia para el sector ferroviario y, a la hora de aplicar medidas de resiliencia en virtud de la presente Directiva, se anima a las entidades críticas a que se remitan a las directrices no vinculantes y documentos de buenas prácticas elaborados en el marco de líneas de trabajo sectoriales, como la Plataforma de la UE en materia de seguridad de los viajeros de ferrocarril establecida por la Decisión 2018/C 232/03 de la Comisión ([18]).

(32) El riesgo de que los empleados de las entidades críticas o sus contratistas hagan un uso indebido, por ejemplo, de sus derechos de acceso dentro de la organización de la entidad crítica para causar daños y perjuicios es cada vez más preocupante. Por tanto, los Estados miembros deben especificar las condiciones en las cuales las entidades críticas están autorizadas, en casos debidamente motivados y teniendo en cuenta las evaluaciones de riesgos del Estado miembro, para presentar solicitudes de comprobación de antecedentes personales de las personas pertenecientes a categorías específicas de su personal. Debe garantizarse que las autoridades competentes evalúen dichas solicitudes en un plazo razonable, y las tramiten de conformidad con el Derecho y los procedimientos nacionales y con el Derecho de la Unión pertinente y aplicable, también en materia de protección de datos personales. A fin de corroborar la identidad de una persona objeto de una comprobación de antecedentes personales, conviene que los Estados miembros exijan una prueba de identidad, como un pasaporte, un documento nacional de identidad o formas digitales de identificación, de conformidad con el Derecho aplicable.

([14]) 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).

([15]) 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).

([16]) 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).

([17]) Directiva 2008/96/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre gestión de la seguridad de las infraestructuras viarias (DO L 319 de 29.11.2008, p. 59).

([18]) Decisión de la Comisión, de 29 de junio de 2018, por la que se establece la Plataforma de la UE en materia de seguridad de los viajeros de ferrocarril 2018/C 232/03 (DO C 232 de 3.7.2018, p. 10).

Las comprobaciones de antecedentes personales deben incluir una comprobación de los registros de antecedentes penales de la persona de que se trate. Los Estados miembros deben utilizar información procedente del Sistema Europeo de Información de Antecedentes Penales, de conformidad con los procedimientos establecidos en la Decisión Marco 2009/315/JAI del Consejo ([19]) y, cuando proceda y sea aplicable, en el Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo ([20]), a fin de obtener información de los registros de antecedentes penales de otros Estados miembros. Los Estados miembros también podrían recurrir, cuando proceda y sea aplicable, al Sistema de Información de Schengen de segunda generación (SIS II) establecido por el Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo ([21]), a la inteligencia, así como a cualquier otra información objetiva disponible que pueda ser necesaria para determinar la idoneidad de la persona de que se trate para trabajar en el puesto para el cual la entidad crítica haya solicitado una comprobación de antecedentes personales.

(33) Debe establecerse un mecanismo para la notificación de determinados incidentes que permita a las autoridades competentes responder a los incidentes de forma rápida y adecuada, y tener una visión global de las repercusiones, la naturaleza, la causa y las posibles consecuencias de un incidente al que se enfrenten las entidades críticas. Las entidades críticas deben notificar sin demora indebida a las autoridades competentes los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales. A menos que sean operativamente incapaces de hacerlo, las entidades críticas deben presentar una notificación inicial a más tardar veinticuatro horas después de haber tenido conocimiento de un incidente. La notificación inicial únicamente debe incluir la información que sea estrictamente necesaria para que la autoridad competente tenga constancia del incidente y la entidad crítica pueda solicitar asistencia, en caso de que sea necesario. Dicha notificación debe indicar, en la medida de lo posible, la causa presunta del incidente. Los Estados miembros deben asegurarse de que el requisito de presentar dicha notificación inicial no desvíe los recursos de la entidad crítica de actividades relacionadas con la gestión de incidentes que deban priorizarse. La notificación inicial debe ir seguida, en su caso, de un informe detallado a más tardar un mes después del incidente. El informe detallado debe complementar la notificación inicial y ofrecer una visión más completa del incidente.

(34) La normalización debe seguir siendo un proceso impulsado fundamentalmente por el mercado. Sin embargo, aún pueden darse situaciones en las que sea conveniente exigir el cumplimiento de normas específicas. Cuando resulte útil, los Estados miembros deben fomentar la aplicación de normas y especificaciones técnicas europeas e internacionales que sean pertinentes para las medidas de seguridad y resiliencia aplicables a las entidades críticas.

(35) Si bien las entidades críticas actúan generalmente como parte de una red cada vez más interconectada de prestación de servicios e infraestructuras y a menudo prestan servicios esenciales en más de un Estado miembro, algunas de dichas entidades revisten especial importancia para la Unión y su mercado interior, ya que prestan servicios esenciales a o en seis o más Estados miembros y, por lo tanto, podrían beneficiarse de apoyo específico a escala de la Unión. Por consiguiente, deben establecerse normas sobre las misiones de asesoramiento con respecto de dichas entidades críticas de especial importancia europea. Dichas normas se entenderán sin perjuicio de las normas sobre supervisión y ejecución establecidas en la presente Directiva.

(36) Previa solicitud motivada de la Comisión o de uno o más Estados miembros a o en los que se preste el servicio esencial, cuando se necesite información adicional para poder asesorar a una entidad crítica en el cumplimiento de sus obligaciones en virtud de la presente Directiva o para evaluar si una entidad crítica de especial importancia europea cumple las citadas obligaciones, el Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica debe entregar a la Comisión determinada información según lo dispuesto en la presente Directiva. De acuerdo con el Estado miembro que haya identificado como entidad crítica a la entidad crítica de especial importancia europea, la Comisión debe poder organizar una misión de asesoramiento para evaluar las medidas adoptadas por dicha entidad. A fin de garantizar que estas misiones de asesoramiento se lleven a cabo correctamente, deben establecerse normas complementarias, en particular sobre la organización y realización de las misiones de asesoramiento, el seguimiento que deba darse y las obligaciones de las entidades críticas de especial importancia europea de que se trate. Las misiones de asesoramiento deben llevarse a cabo, sin perjuicio de

([19]) Decisión Marco 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L 93 de 7.4.2009, p. 23).

([20]) Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-NTP) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

([21]) Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

la necesidad de que el Estado miembro donde se realicen y la entidad crítica interesada cumplan las normas establecidas en la presente Directiva, de conformidad con las normas detalladas del Derecho de dicho Estado miembro, por ejemplo, sobre las condiciones precisas que deben cumplirse a fin de tener acceso a las instalaciones o documentos pertinentes y sobre las vías de recurso judicial. Los conocimientos específicos necesarios para estas misiones de asesoramiento podrían solicitarse, cuando proceda, a través del Centro de Coordinación de la Respuesta a Emergencias establecido por la Decisión n.º 1313/2013/UE del Parlamento Europeo y del Consejo ([22]).

(37) Con el fin de apoyar a la Comisión y facilitar la cooperación entre los Estados miembros y el intercambio de información, incluidas las mejores prácticas, sobre las cuestiones relacionadas con la presente Directiva, debe establecerse un Grupo de Resiliencia de las Entidades Críticas, en calidad de grupo de expertos de la Comisión. Los Estados miembros deben procurar garantizar que los representantes designados de sus autoridades competentes en el Grupo de Resiliencia de las Entidades Críticas cooperen de manera eficaz y eficiente, también mediante el nombramiento de representantes que cuenten con la habilitación de seguridad, en su caso. El Grupo de Resiliencia de las Entidades Críticas comenzará a desempeñar sus funciones tan pronto como sea posible a fin de proporcionar medios adicionales para una cooperación adecuada durante el período de transposición de la presente Directiva. El Grupo de Resiliencia de las Entidades Críticas debe interactuar con otros grupos de expertos sectoriales pertinentes.

(38) El Grupo de Resiliencia de las Entidades Críticas debe cooperar con el Grupo de Cooperación establecido en virtud de la Directiva (UE) 2022/2555 con vistas a apoyar un marco global para la resiliencia cibernética y no cibernética de las entidades críticas. El Grupo de Resiliencia de las Entidades Críticas y el Grupo de Cooperación establecido en virtud de la Directiva (UE) 2022/2555 deben entablar un diálogo periódico a fin de promover la cooperación entre las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555, y de facilitar el intercambio de información, en particular sobre temas de interés para ambos grupos.

(39) A fin de alcanzar los objetivos de la presente Directiva, y sin perjuicio de la responsabilidad jurídica de los Estados miembros y de las entidades críticas de garantizar el cumplimiento de sus respectivas obligaciones establecidas en ella, la Comisión, cuando lo considere oportuno, debe prestar apoyo a las autoridades competentes y entidades críticas con el objetivo de facilitarles el cumplimiento de sus respectivas obligaciones. Al prestar apoyo a los Estados miembros y a las entidades críticas en el cumplimiento de las obligaciones derivadas de la presente Directiva, la Comisión debe basarse en las estructuras e instrumentos existentes, como el Mecanismo de Protección Civil de la Unión, creado por la Decisión n.º 1313/2013/UE, y la Red Europea de Referencia para la Protección de Infraestructuras Críticas. Además, debe informar a los Estados miembros de los recursos disponibles a escala de la Unión, como el Fondo de Seguridad Interior, creado por el Reglamento (UE) 2021/1149 del Parlamento Europeo y del Consejo ([23]), Horizonte Europa, creado por el Reglamento (UE) 2021/695 del Parlamento Europeo y del Consejo ([24]), u otros instrumentos pertinentes para la resiliencia de las entidades críticas.

(40) Los Estados miembros deben garantizar que sus autoridades competentes dispongan de determinadas facultades específicas para la correcta aplicación y ejecución de la presente Directiva en relación con las entidades críticas, cuando tales entidades estén sujetas a su jurisdicción según lo dispuesto en la presente Directiva. Dichas competencias deben incluir, en particular, la facultad de realizar inspecciones y auditorías, la facultad de supervisar, la facultad de exigir a las entidades críticas que faciliten información y pruebas sobre las medidas que hayan adoptado para cumplir sus obligaciones y, en caso necesario, la facultad de emitir órdenes para subsanar los incumplimientos detectados. Al emitir tales órdenes, los Estados miembros no deben exigir la adopción de medidas que vayan más allá de lo necesario y proporcionado para garantizar el cumplimiento de la entidad crítica de que se trate, teniendo en cuenta, en particular, la gravedad del incumplimiento y la capacidad económica de dicha entidad crítica. En términos más generales, estas competencias deben ir acompañadas de garantías adecuadas y eficaces que

([22]) 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).

([23]) Reglamento (UE) 2021/1149 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se crea el Fondo de Seguridad Interior (DO L 251 de 15.7.2021, p. 94).

([24]) Reglamento (UE) 2021/695 del Parlamento Europeo y del Consejo, de 28 de abril de 2021, por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa», se establecen sus normas de participación y difusión, y se derogan los Reglamentos (UE) n.º 1290/2013 y (UE) n.º 1291/2013 (DO L 170 de 12.5.2021, p. 1).

se especificarán en el Derecho nacional de conformidad con la Carta de los Derechos Fundamentales de la Unión Europea. Al evaluar el cumplimiento por parte de una entidad crítica de sus obligaciones tal como se establece en la presente Directiva, las autoridades competentes con arreglo a la presente Directiva deben poder solicitar a las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 que ejerzan sus facultades de supervisión y ejecución en relación con una entidad con arreglo a dicha Directiva que haya sido identificada como entidad crítica con arreglo a la presente Directiva. Las autoridades competentes con arreglo a la presente Directiva y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 deben cooperar e intercambiar información a tal efecto.

(41) A fin de aplicar la presente Directiva de manera eficaz y coherente, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE con el fin de completar la presente Directiva mediante la elaboración de una lista de servicios esenciales. Las autoridades competentes deben utilizar dicha lista para realizar las evaluaciones de riesgos del Estado miembro e identificar las entidades críticas con arreglo a la presente Directiva. A la luz del enfoque de armonización mínima de la presente Directiva, dicha lista no es exhaustiva y los Estados miembros podrían complementarla con servicios esenciales adicionales a nivel nacional a fin de tener en cuenta las características específicas nacionales en la prestación de servicios esenciales. 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 ([25]). 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.

(42) A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([26]).

(43) Dado que los objetivos de la presente Directiva, a saber, garantizar la prestación sin obstrucciones en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales y aumentar la resiliencia de las entidades críticas que prestan tales servicios, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a los efectos de la acción, pueden 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 artículo 5, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

(44) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([27]), emitió su dictamen el 11 de agosto de 2021.

(45) Por consiguiente, debe derogarse la Directiva 2008/114/CE.

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

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

([27]) 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).

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva:

a) obliga a los Estados miembros a adoptar medidas específicas destinadas a garantizar la prestación sin obstrucciones en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales dentro del ámbito de aplicación del artículo 114 del TFUE, en particular las obligaciones de identificar las entidades críticas y de apoyarlas en el cumplimiento de las obligaciones impuestas a estas últimas;

b) establece obligaciones a fin de que las entidades críticas aumenten su resiliencia y capacidad de prestar los servicios mencionados en la letra a) en el mercado interior;

c) establece normas:

i) sobre la supervisión de las entidades críticas,

ii) sobre la ejecución,

iii) para la identificación de las entidades críticas de especial importancia europea y sobre misiones de asesoramiento para evaluar las medidas adoptadas por tales entidades con el fin de cumplir sus obligaciones con arreglo al capítulo III;

d) establece procedimientos comunes de cooperación e información sobre la aplicación de la presente Directiva;

e) establece medidas con vistas a lograr un alto nivel de resiliencia de las entidades críticas a fin de garantizar la prestación de servicios esenciales dentro de la Unión y mejorar el funcionamiento del mercado interior.

2. La presente Directiva no se aplicará a las materias reguladas por la Directiva (UE) 2022/2555, sin perjuicio de lo dispuesto en el artículo 8 de la presente Directiva. Habida cuenta de la relación entre la seguridad física y la ciberseguridad de las entidades críticas, los Estados miembros garantizarán que la presente Directiva y la Directiva (UE) 2022/2555 se apliquen de manera coordinada.

3. Las disposiciones pertinentes de la presente Directiva, incluidas las disposiciones sobre supervisión y ejecución establecidas en el capítulo VI, no serán de aplicación en caso de que las disposiciones de actos jurídicos sectoriales de la Unión obliguen a las entidades críticas a adoptar medidas para aumentar su resiliencia y cuando tales obligaciones sean reconocidas por los Estados miembros como al menos equivalentes a las obligaciones correspondientes establecidas en la presente Directiva.

4. 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 pertinentes de conformidad con la presente Directiva únicamente cuando tal intercambio sea necesario para 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 la seguridad y los intereses comerciales de las entidades críticas, respetando al mismo tiempo la seguridad de los Estados miembros.

5. La presente Directiva se entenderá sin perjuicio de la responsabilidad de los Estados miembros de salvaguardar la seguridad nacional y la defensa y de su competencia para salvaguardar otras funciones esenciales del Estado, como garantizar la integridad territorial del Estado y mantener el orden público.

6. La presente Directiva no se aplicará a entidades de la administración pública que realicen sus actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación de la ley, con inclusión de la investigación, la detección y el enjuiciamiento de infracciones penales.

7. Los Estados miembros podrán decidir que el artículo 11 y los capítulos III, IV y VI, en parte o en su totalidad, no se apliquen a entidades críticas específicas que realizan actividades en los ámbitos de la seguridad nacional, la seguridad pública, la defensa o la aplicación de la ley, con inclusión de la investigación, la detección y el enjuiciamiento de infracciones penales, o que presten servicios exclusivamente a las entidades de la administración pública a que hace referencia el apartado 6 del presente artículo.

8. Las obligaciones establecidas en la presente Directiva no implicarán el suministro de información cuya divulgación fuera contraria a los intereses esenciales de seguridad nacional, seguridad pública o defensa de los Estados miembros.

9. La presente Directiva se entiende sin perjuicio del Derecho de la Unión en materia de protección de datos personales, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([28]) y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([29]).

Artículo 2

Definiciones

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

1) «entidad crítica»: una entidad pública o privada identificada por un Estado miembro de conformidad con el artículo 6 como perteneciente a una de las categorías establecidas en la tercera columna del cuadro del anexo;

2) «resiliencia»: la capacidad de una entidad crítica para la prevención, la protección, la respuesta, la resistencia, la mitigación, la absorción, la adaptación y la recuperación en caso de un incidente;

3) «incidente»: un acontecimiento que tiene el potencial de perturbar significativamente, o que perturbe, la prestación de un servicio esencial, en particular cuando afecte a los sistemas nacionales que salvaguardan el Estado de Derecho;

4) «infraestructura crítica»: un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que es necesario para la prestación de un servicio esencial;

5) «servicio esencial»: un servicio que es crucial para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud pública y la seguridad, o el medio ambiente;

6) «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;

7) «evaluación de riesgos»: el proceso general dirigido a determinar la naturaleza y el alcance de un riesgo mediante la identificación y el análisis de potenciales amenazas, vulnerabilidades y peligros pertinentes que puedan dar lugar a un incidente y mediante la evaluación de las posibles pérdidas o perturbaciones en la prestación de un servicio esencial causadas por dicho incidente;

8) «norma»: una norma tal como se define en el artículo 2, apartado 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([30]);

([28]) 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).

([29]) 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).

([30]) 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).

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

10) «entidad de la administración pública»: una entidad reconocida como tal en un Estado miembro de conformidad con el Derecho nacional, con excepción del poder judicial, los parlamentos o 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 autoridades estatales u otras entidades de Derecho público a nivel central, cuya gestión se halla sometida a un control por parte de estas autoridades o entidades, o tiene órganos de administración, de dirección o de supervisión más de la mitad de cuyos miembros los nombran las autoridades estatales u otras entidades de Derecho público a nivel central;

d) esté facultada para dirigir a las personas físicas o jurídicas resoluciones administrativas o reglamentarias que afecten a sus derechos en la circulación transfronteriza de personas, mercancías, servicios o capitales.

Artículo 3

Armonización mínima

La presente Directiva no será óbice para que los Estados miembros adopten o mantengan disposiciones de Derecho nacional con el objeto de alcanzar un mayor nivel de resiliencia de las entidades críticas, siempre y cuando tales disposiciones sean compatibles con las obligaciones que el Derecho de la Unión impone a los Estados miembros.

CAPÍTULO II

MARCOS NACIONALES PARA LA RESILIENCIA DE LAS ENTIDADES CRITICAS

Artículo 4

Estrategia para la resiliencia de las entidades críticas

1. Tras una consulta que, en la medida de lo posible, esté abierta a las partes interesadas pertinentes, cada Estado miembro adoptará a más tardar el 17 de enero de 2026 una estrategia para aumentar la resiliencia de las entidades críticas (en lo sucesivo, «estrategia»). La estrategia establecerá objetivos estratégicos y medidas de actuación, basándose en estrategias nacionales y sectoriales, planes o documentos similares existentes en la materia, con vistas a alcanzar y mantener un alto nivel de resiliencia por parte de las entidades críticas y abarcará, como mínimo, los sectores indicados en el anexo.

2. Cada estrategia incluirá, como mínimo, los elementos siguientes:

a) los objetivos estratégicos y las prioridades con el fin de aumentar la resiliencia global de las entidades críticas, teniendo en cuenta las dependencias e interdependencias transfronterizas e intersectoriales;

b) un marco de gobernanza para alcanzar los objetivos estratégicos y las prioridades, incluida una descripción de las funciones y responsabilidades de las diferentes autoridades, entidades críticas y otras partes implicadas en la aplicación de la estrategia;

c) una descripción de las medidas necesarias para aumentar la resiliencia global de las entidades críticas, incluida una descripción de la evaluación de riesgos a que se refiere el artículo 5;

d) una descripción del proceso por el que se identifican las entidades críticas;

e) una descripción del proceso de apoyo a las entidades críticas de conformidad con el presente capítulo, incluidas las medidas para mejorar la cooperación entre el sector público, por una parte, y el sector privado y las entidades públicas y privadas, por otra;

f) una lista de las principales autoridades y partes interesadas pertinentes, distintas de las entidades críticas, que participen en la ejecución de la estrategia;

g) un marco de actuación a efectos de la coordinación entre las autoridades competentes con arreglo a la presente Directiva (en lo sucesivo, «autoridades competentes») y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 a efectos del intercambio de información sobre los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella y el ejercicio de las tareas de supervisión;

h) una descripción de las medidas ya adoptadas con el fin de facilitar el cumplimiento de las obligaciones con arreglo al capítulo III de la presente Directiva por parte de las pequeñas y medianas empresas en el sentido del anexo de la Recomendación 2003/361/CE de la Comisión ([31]) identificadas como entidades críticas por el Estado miembro en cuestión.

Tras una consulta que, en la medida de lo posible, esté abierta a las partes interesadas pertinentes, los Estados miembros actualizarán sus estrategias como mínimo cada cuatro años.

3. Los Estados miembros comunicarán a la Comisión sus estrategias, así como sus actualizaciones sustanciales, en el plazo de tres meses a partir de la fecha de su adopción.

Artículo 5

Evaluación de riesgos por los Estados miembros

1. La Comisión estará facultada para adoptar un acto delegado con arreglo al artículo 23, a más tardar el 17 de noviembre de 2023, que complete la presente Directiva mediante el establecimiento de una lista no exhaustiva de servicios esenciales en los sectores y subsectores indicados en el anexo. Las autoridades competentes recurrirán a dicha lista con el fin de realizar una evaluación de riesgos (en lo sucesivo, «evaluación de riesgos del Estado miembro») a más tardar el 17 de enero de 2026, y posteriormente siempre que sea necesario y como mínimo cada cuatro años. Las autoridades competentes utilizarán las evaluaciones de riesgos del Estado miembro con el fin de identificar las entidades críticas de conformidad con el artículo 6 y ayudar a dichas entidades críticas a adoptar medidas con arreglo al artículo 13.

Las evaluaciones de riesgos del Estado miembro tendrán en cuenta los riesgos naturales y de origen humano pertinentes, incluidos los de naturaleza intersectorial o transfronteriza, los accidentes, las catástrofes naturales, las emergencias de salud pública y las amenazas híbridas u otras amenazas antagónicas, incluidos los delitos de terrorismo s según lo dispuesto en la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo ([32]).

2. Al realizar las evaluaciones de riesgos del Estado miembro, los Estados miembros tendrán en cuenta como mínimo lo siguiente:

a) la evaluación general de riesgos realizada de conformidad con el artículo 6, apartado 1, de la Decisión n.º 1313/2013/UE;

b) otras evaluaciones de riesgos pertinentes realizadas de conformidad con los requisitos de los actos jurídicos sectoriales de la Unión pertinentes, incluidos los Reglamentos (UE) 2017/1938 ([33]) y (UE) 2019/941 ([34]) del Parlamento Europeo y del Consejo y las Directivas 2007/60/CE ([35]) y 2012/18/UE ([36]) del Parlamento Europeo y del Consejo;

([31]) 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).

([32]) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO L 88 de 31.3.2017, p. 6).

([33]) Reglamento (UE) 2017/1938 del Parlamento Europeo y del Consejo, de 25 de octubre de 2017, sobre medidas para garantizar la seguridad del suministro de gas y por el que se deroga el Reglamento (UE) n.º 994/2010 (DO L 280 de 28.10.2017, p. 1).

([34]) Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE (DO L 158 de 14.6.2019, p. 1).

([35]) Directiva 2007/60/CE del Parlamento Europeo y del Consejo, de 23 de octubre de 2007, relativa a la evaluación y gestión de los riesgos de inundación (DO L 288 de 6.11.2007, p. 27).

([36]) Directiva 2012/18/UE del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativa al control de los riesgos inherentes a los accidentes graves en los que intervengan sustancias peligrosas y por la que se modifica y ulteriormente deroga la Directiva 96/82/CE (DO L 197 de 24.7.2012, p. 1).

c) los riesgos pertinentes derivados del grado de interdependencia de los sectores indicados en el anexo, incluido el grado en que dependen de entidades situadas en otros Estados miembros y terceros países, y las repercusiones que una perturbación significativa en un sector pueda tener en otros sectores, incluido cualquier riesgo significativo para los ciudadanos y el mercado interior;

d) cualquier información sobre incidentes notificados de conformidad con el artículo 15.

A efectos del párrafo primero, letra c), los Estados miembros cooperarán con las autoridades competentes de otros Estados miembros y las autoridades competentes de terceros países, según proceda.

3. Los Estados miembros pondrán los elementos pertinentes de las evaluaciones de riesgos del Estado miembro a disposición de las entidades críticas que los Estados miembros hayan identificado con arreglo al artículo 6, a través, cuando proceda, de sus puntos de contacto únicos. Los Estados miembros garantizarán que la información facilitada a las entidades críticas ayude a estas en la realización de sus evaluaciones de riesgos de conformidad con el artículo 12 y en la adopción de medidas para garantizar su resiliencia de conformidad con el artículo 13.

4. En un plazo de tres meses tras la realización de la evaluación de riesgos del Estado miembro, este facilitará a la Comisión información pertinente sobre los tipos de riesgos determinados a raíz de dicha evaluación y los resultados de esta, por sectores y subsectores indicados en el anexo.

5. La Comisión, en cooperación con los Estados miembros, elaborará un modelo común voluntario de presentación de informes a efectos del cumplimiento de lo dispuesto en el apartado 4.

Artículo 6

Identificación de las entidades críticas

1. A más tardar el 17 de julio de 2026, los Estados miembros identificarán las entidades críticas para los sectores y subsectores indicados en el anexo.

2. Cuando un Estado miembro identifique entidades críticas con arreglo al apartado 1, tendrá en cuenta los resultados de su evaluación de riesgos del Estado miembro y su estrategia y aplicará todos los criterios siguientes:

a) la entidad presta uno o más servicios esenciales;

b) la entidad opera en el territorio de dicho Estado miembro y su infraestructura crítica está situada en él, y

c) un incidente tendría efectos perturbadores significativos, determinados de conformidad con el artículo 7, apartado 1, en la prestación por la entidad de uno o más servicios esenciales, o en la prestación de otros servicios esenciales en los sectores indicados en el anexo que dependen de dicho o dichos servicios esenciales.

3. Cada Estado miembro elaborará una lista de las entidades críticas identificadas con arreglo al apartado 2 y garantizará que se les notifique, en el plazo de un mes a partir de su identificación, que han sido identificadas como entidades críticas. Los Estados miembros informarán a esas entidades críticas de las obligaciones que les incumben con arreglo a los capítulos III y IV y de la fecha a partir de la cual dichas obligaciones les son aplicables, sin perjuicio de lo dispuesto en el artículo 8. Los Estados miembros informarán a las entidades críticas en los sectores indicados en los puntos 3, 4 y 8 del cuadro del anexo de que no están sometidas a ninguna obligación con arreglo a los capítulos III y IV, a menos que las medidas nacionales dispongan otra cosa.

El capítulo III se aplicará a las entidades críticas de que se trate a partir de diez meses después de la fecha de la notificación a que se refiere el párrafo primero del presente apartado.

4. Los Estados miembros garantizarán que sus autoridades competentes con arreglo a la presente Directiva notifiquen a las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 la identidad de las entidades críticas que hayan identificado con arreglo al presente artículo, en el plazo de un mes a partir de la identificación. Dicha notificación especificará, cuando proceda, que las entidades críticas de que se trate son entidades de los sectores indicados en los puntos 3, 4 y 8 del cuadro anexo de la presente Directiva y que no están sometidas a ninguna obligación con arreglo a sus capítulos III y IV.

5. Cuando sea necesario y, en cualquier caso, como mínimo cada cuatro años, los Estados miembros revisarán y, en su caso, actualizarán la lista de las entidades críticas identificadas a que se refiere el apartado 3. Cuando tales actualizaciones conduzcan a la identificación de entidades críticas adicionales, los apartados 3 y 4 se aplicarán a dichas entidades críticas adicionales. Además, los Estados miembros garantizarán que las entidades que, después de tal actualización, ya no estén identificadas como entidades críticas reciban a su debido tiempo la notificación a este respecto y de que ha dejado de estar sometidas a las obligaciones con arreglo al capítulo III desde la fecha de recepción de dicha notificación.

6. La Comisión, en cooperación con los Estados miembros, elaborará recomendaciones y directrices no vinculantes con el fin de ayudar a estos últimos a identificar entidades críticas.

Artículo 7

Efecto perturbador significativo

1. Al determinar el carácter significativo de un efecto perturbador a que se refiere el artículo 6, apartado 2, letra c), los Estados miembros tendrán en cuenta los criterios siguientes:

a) el número de usuarios que dependen del servicio esencial prestado por la entidad de que se trate;

b) el grado en que otros sectores y subsectores indicados en el anexo dependen del servicio esencial en cuestión;

c) las repercusiones que los incidentes podrían tener, en términos de grado y duración, en las actividades económicas y sociales, el medio ambiente, la seguridad y la protección públicas o la salud de la población;

d) la cuota de mercado de la entidad en el mercado del servicio o servicios esenciales de que se trate;

e) la zona geográfica que podría verse afectada por un incidente, incluido cualquier repercusión transfronteriza, teniendo en cuenta la vulnerabilidad asociada al grado de aislamiento de ciertos tipos de zonas geográficas, como las regiones insulares, las regiones remotas o las zonas montañosas;

f) la importancia de la entidad para mantener un nivel suficiente de servicio esencial, teniendo en cuenta la disponibilidad de medios alternativos para la prestación de dicho servicio esencial.

2. Una vez identificadas las entidades críticas con arreglo al artículo 6, apartado 1, cada Estado miembro presentará a la Comisión sin demora indebida la siguiente información:

a) una lista de servicios esenciales en ese Estado miembro en caso de contar con servicios esenciales adicionales en comparación con la lista de servicios esenciales a que se refiere el artículo 5, apartado 1;

b) el número de entidades críticas identificadas para cada sector y subsector indicado en el anexo y para cada servicio esencial;

c) los umbrales aplicados para especificar uno o varios de los criterios del apartado 1.

Los umbrales a que se refiere el párrafo primero, letra c), podrán presentarse como tales o de forma agregada.

Los Estados miembros presentarán posteriormente la información indicada en el párrafo primero en caso de que sea necesario y como mínimo cada cuatro años.

3. La Comisión, previa consulta al Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19, adoptará directrices no vinculantes para facilitar la aplicación de los criterios a que se refiere el apartado 1 del presente artículo, teniendo en cuenta la información a que se refiere el apartado 2 del presente artículo.

Artículo 8

Entidades críticas del sector bancario, de las infraestructuras de los mercados financieros y de las infraestructuras digitales

Los Estados miembros se asegurarán de que el artículo 11 y los capítulos III, IV y VI no se apliquen a las entidades críticas que hayan identificado en los sectores indicados en los puntos 3, 4 y 8 del cuadro del anexo. Los Estados miembros podrán adoptar o mantener disposiciones de Derecho nacional a fin de alcanzar un mayor nivel de resiliencia de dichas entidades críticas, a condición de que tales disposiciones sean coherentes con el Derecho de la Unión aplicable.

Artículo 9

Autoridades competentes y punto de contacto único

1. Cada Estado miembro designará o establecerá una o varias autoridades competentes responsables de la correcta aplicación y, en caso necesario, ejecución a escala nacional de las disposiciones establecidas en la presente Directiva.

Con respecto a las entidades críticas en los sectores indicados en los puntos 3 y 4 del cuadro del anexo de la presente Directiva, las autoridades competentes serán, en principio, las autoridades competentes a que se refiere el artículo 46 del Reglamento (UE) 2022/2554. Con respecto a las entidades críticas en el sector indicado en el punto 8 del cuadro del anexo de la presente Directiva, las autoridades competentes serán, en principio, las autoridades competentes con arreglo a la Directiva (UE) 2022/2555. Los Estados miembros podrán designar una autoridad competente diferente para los sectores indicados en los puntos 3, 4 y 8 del cuadro del anexo de la presente Directiva, de conformidad con los marcos nacionales vigentes.

Cuando designen o establezcan más de una autoridad competente, los Estados miembros fijarán claramente las tareas de cada una de las autoridades interesadas y se asegurarán de que cooperen eficazmente para desempeñar las funciones con arreglo a la presente Directiva, también en lo que se refiere a la designación y las actividades del punto de contacto único a que se refiere el apartado 2.

2. Cada Estado miembro designará o establecerá un punto de contacto único para que ejerza una función de enlace con el fin de garantizar la cooperación transfronteriza con los puntos de contacto únicos de otros Estados miembros y con el Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19 (en lo sucesivo, «punto de contacto único»). Cuando proceda, el Estado miembro designará su punto de contacto único en el seno de una autoridad competente. Cuando proceda, el Estados miembro podrá disponer que su punto de contacto único también ejerza una función de enlace con la Comisión y garantice la cooperación con terceros países.

3. A más tardar el 17 de julio de 2028, y posteriormente cada dos años, los puntos de contacto únicos presentarán a la Comisión y al Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19 un informe de síntesis sobre las notificaciones recibidas, incluido el número de notificaciones, la naturaleza de los incidentes notificados y las medidas adoptadas de conformidad con el artículo 15, apartado 3.

La Comisión, en cooperación con el Grupo de Resiliencia de las Entidades Críticas, elaborará un modelo común para la presentación de informes. Las autoridades competentes podrán utilizar con carácter voluntario dicho modelo común para la presentación de los informes de síntesis a que se refiere el párrafo primero.

4. Cada Estado miembro garantizará que su autoridad competente y el punto de contacto único tengan las competencias y los recursos financieros, humanos y técnicos adecuados para llevar a cabo, de manera eficaz y eficiente, las tareas que se les asignen.

5. Cada Estado miembro garantizará que su autoridad competente, cuando proceda y de conformidad con el Derecho de la Unión y nacional aplicable, consulte y coopere con otras autoridades nacionales pertinentes, incluidas las encargadas de la protección civil, la aplicación de la ley y la protección de datos personales, así como con las entidades críticas y las partes interesadas pertinentes.

6. Cada Estado miembro garantizará que su autoridad competente con arreglo a la presente Directiva coopere e intercambie información con las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 en relación con los riesgos, amenazas e incidentes relacionados con la ciberseguridad y los riesgos, amenazas e incidentes no relacionados con ella que afecten a entidades críticas, así como sobre las medidas pertinentes adoptadas por su autoridad competente y las autoridades competentes con arreglo a la Directiva (UE) 2022/2555.

7. En el plazo de tres meses a partir de la designación o el establecimiento de la autoridad competente y del punto de contacto único, cada Estado miembro notificará a la Comisión su identidad y sus tareas y responsabilidades con arreglo a la presente Directiva, así como sus datos de contacto y cualquier modificación posterior de estos. Los Estados miembros informarán a la Comisión en caso de que decidan designar autoridades competentes en relación con las entidades críticas en los sectores indicados en los puntos 3, 4 y 8 del cuadro del anexo a una autoridad distinta de las autoridades competentes a que se refiere el apartado 1, párrafo segundo. Cada Estado miembro hará pública la identidad de su autoridad competente y punto de contacto único.

8. La Comisión elaborará una lista de los puntos de contacto únicos de acceso público.

Artículo 10

Apoyo de los Estados miembros a las entidades críticas

1. Los Estados miembros ayudarán a las entidades críticas a aumentar su resiliencia. Este apoyo podrá incluir el desarrollo de materiales y metodologías de orientación, el apoyo a la organización de ejercicios para probar su resiliencia y la prestación de asesoramiento y formación al personal de las entidades críticas. Sin perjuicio de las normas aplicables en materia de ayudas estatales, los Estados miembros podrán proporcionar recursos financieros a las entidades críticas cuando sea necesario y esté justificado por objetivos de interés público.

2. Cada Estado miembro garantizará que su autoridad competente coopere e intercambie información y buenas prácticas con las entidades críticas de los sectores indicados en el anexo.

3. Los Estados miembros facilitarán el intercambio voluntario de información entre las entidades críticas en relación con las materias reguladas por la presente Directiva, de conformidad con el Derecho de la Unión y nacional, en particular sobre información clasificada y delicada, competencia y protección de datos personales.

Artículo 11

Cooperación entre los Estados miembros

1. Cuando proceda, los Estados miembros se consultarán mutuamente en relación con las entidades críticas con el fin de garantizar que la presente Directiva se aplique de manera coherente. Dichas consultas tendrán lugar, en particular, en relación con las entidades críticas que:

a) utilicen infraestructuras críticas que estén físicamente conectadas entre dos o más Estados miembros;

b) formen parte de estructuras corporativas que estén conectadas o vinculadas a entidades críticas de otros Estados miembros;

c) hayan sido identificadas como entidades críticas en un Estado miembro y presten servicios esenciales a otros Estados miembros o en otros Estados miembros.

2. Las consultas a que se refiere el apartado 1 tendrán como objetivo aumentar la resiliencia de las entidades críticas y, en la medida de lo posible, reducir la carga administrativa que soportan.

CAPÍTULO III

RESILIENCIA DE LAS ENTIDADES CRÍTICAS

Artículo 12

Evaluación de riesgos por parte de las entidades críticas

1. No obstante el plazo establecido en el artículo 6, apartado 3, párrafo segundo, los Estados miembros garantizarán que las entidades críticas realicen una evaluación de riesgos en el plazo de nueve meses a partir de la recepción de la notificación a que se refiere el artículo 6, apartado 3, y posteriormente siempre que sea necesario y como mínimo cada cuatro años, sobre la base de las evaluaciones de riesgos del Estado miembro y otras fuentes de información pertinentes, a fin de evaluar todos los riesgos pertinentes que puedan perturbar la prestación de sus servicios esenciales (en lo sucesivo, «evaluación de riesgos de la entidad crítica»).

2. La evaluación de riesgos de la entidad crítica tendrá en cuenta los riesgos naturales y de origen humano pertinentes que puedan dar lugar a un incidente, entre ellos los de naturaleza intersectorial o transfronteriza, los accidentes, las catástrofes naturales, las emergencias de salud pública y las amenazas híbridas y otras amenazas antagónicas, incluidos los delitos de terrorismo establecidos en la Directiva (UE) 2017/541. La evaluación de riesgos de la entidad crítica tendrá en cuenta el grado en que otros sectores indicados en el anexo dependen del servicio esencial prestado por dicha entidad crítica y el grado en que esta depende de otros servicios esenciales prestados por otras entidades en esos otros sectores, también, cuando proceda, en Estados miembros vecinos y terceros países.

Cuando haya realizado otras evaluaciones de riesgos o elaborado documentos en virtud de obligaciones establecidas en otros actos jurídicos que sean pertinentes para su evaluación de riesgos de la entidad crítica, la entidad crítica podrá utilizar esas otras evaluaciones y documentos para cumplir los requisitos establecidos en el presente artículo. En el ejercicio de sus funciones de supervisión, la autoridad competente podrá declarar conforme, total o parcialmente, con las obligaciones en virtud del presente artículo una evaluación de riesgos existente realizada por una entidad crítica que aborde los riesgos y el grado de dependencia a que se refiere el párrafo primero del presente apartado.

Artículo 13

Medidas de resiliencia de las entidades críticas

1. Los Estados miembros se asegurarán de que las entidades críticas adopten medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas para garantizar su resiliencia, sobre la base de la información pertinente aportada por ellos en la evaluación de riesgos del Estado miembro y de los resultados de la evaluación de riesgos de la entidad crítica, incluidas las medidas necesarias para:

a) evitar que se produzcan incidentes, considerando con la debida atención medidas de reducción del riesgo de catástrofes y de adaptación al cambio climático;

b) garantizar una protección física adecuada de sus instalaciones y de la infraestructura crítica, considerando con la debida atención, a título de ejemplo, las vallas, las barreras, las herramientas y rutinas de vigilancia perimetral, los equipos de detección y los controles de acceso;

c) responder y resistir a las consecuencias de los incidentes y mitigarlas, considerando con la debida atención la aplicación de procedimientos y protocolos de gestión de riesgos y crisis y rutinas de alerta;

d) recuperarse de incidentes, considerando con la debida atención medidas de continuidad de las actividades y la identificación de cadenas de suministro alternativas, a fin de retomar la prestación del servicio esencial;

e) garantizar una gestión adecuada de la protección de los empleados, considerando con la debida atención medidas como la determinación de las categorías del personal que ejerce funciones esenciales, el establecimiento de derechos de acceso a instalaciones, infraestructuras críticas e información delicada, el establecimiento de procedimientos de comprobación de antecedentes personales de conformidad con el artículo 14 y la designación de las categorías de personas que están obligadas a someterse a dicha comprobación de antecedentes, así como el establecimiento de requisitos adecuados en materia de formación y cualificaciones;

f) concienciar al personal pertinente acerca de las medidas mencionadas en las letras a) a e), considerando con la debida atención medidas como la organización de cursos de formación y ejercicios y la elaboración de material de información.

A efectos del párrafo primero, letra e), los Estados miembros se asegurarán de que las entidades críticas tengan en cuenta al personal de los proveedores de servicios externos a la hora de establecer categorías de personal que ejerza funciones esenciales.

2. Los Estados miembros se asegurarán de que las entidades críticas tengan y apliquen un plan de resiliencia o documentos equivalentes que describan las medidas adoptadas con arreglo al apartado 1. Cuando hayan elaborado documentos o tomado medidas en virtud de obligaciones establecidas en otros actos jurídicos que sean pertinentes para las medidas a que se refiere el apartado 1, las entidades críticas podrán utilizar dichos documentos y medidas para cumplir los requisitos establecidos en el presente artículo. En el ejercicio de sus funciones de supervisión, la autoridad competente podrá declarar conformes, total o parcialmente, con las obligaciones establecidas en el presente artículo las medidas existentes de mejora de la resiliencia tomadas por una entidad crítica que aborden, de forma adecuada y proporcionada, las medidas técnicas, organizativas y de seguridad y a que se refiere el apartado 1.

3. Los Estados miembros garantizarán que cada entidad crítica designe a un agente de enlace o equivalente como punto de contacto con las autoridades competentes.

4. A petición del Estado miembro que haya identificado la entidad crítica y con el acuerdo de esta, la Comisión organizará misiones de asesoramiento, de conformidad con las disposiciones establecidas en el artículo 18, apartados 6, 8 y 9, para asesorar a la entidad crítica de que se trate en el cumplimiento de sus obligaciones con arreglo al capítulo III. La misión de asesoramiento informará de sus conclusiones a la Comisión, al Estado miembro y a la entidad crítica de que se trate.

5. La Comisión, previa consulta al Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19, adoptará directrices no vinculantes para especificar con más detalle las medidas técnicas, organizativas y de seguridad que se pueden adoptar con arreglo al apartado 1 del presente artículo.

6. La Comisión adoptará actos de ejecución para establecer las especificaciones técnicas y metodológicas necesarias relativas a la aplicación de las medidas a que se refiere el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 24, apartado 2.

Artículo 14

Comprobación de antecedentes

1. Los Estados miembros especificarán las condiciones en las cuales, en casos debidamente motivados y teniendo en cuenta la evaluación de riesgos del Estado miembro, se permita a una entidad crítica presentar solicitudes de comprobación de los antecedentes personales de quienes:

a) desempeñen tareas delicadas en la entidad crítica o para su beneficio, en particular en relación con la resiliencia de la entidad crítica;

b) estén autorizados a disponer de acceso directo o remoto a sus instalaciones, información o sistemas de control, también por lo que respecta a la seguridad de la entidad crítica;

c) estén siendo considerados para su contratación en puestos que cumplan los criterios establecidos en las letras a) o b).

2. Las solicitudes a que se refiere el apartado 1 del presente artículo se evaluarán en un plazo razonable y se tramitarán de conformidad con el Derecho y los procedimientos nacionales y con el Derecho de la Unión pertinente y aplicable, incluidos el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([37]). Estas comprobaciones de antecedentes serán proporcionadas y se limitarán estrictamente a lo necesario. Se realizarán con el único fin de evaluar un posible riesgo para la seguridad de la entidad crítica de que se trate.

3. La comprobación de antecedentes a que se refiere el apartado 1 incluirá, como mínimo, las siguientes tareas:

a) corroborar la identidad de la persona objeto de la comprobación de antecedentes;

b) comprobar en el registro de antecedentes penales de dicha persona la existencia de delitos que sean significativos para un puesto concreto.

Al efectuar las comprobaciones de antecedentes, los Estados miembros utilizarán el Sistema Europeo de Información de Antecedentes Penales de conformidad con los procedimientos establecidos en la Decisión Marco 2009/315/JAI y, cuando proceda y sea aplicable, en el Reglamento (UE) 2019/816 a efectos de la obtención de información del registro de antecedentes penales de otros Estados miembros. Las autoridades centrales a que se refieren el artículo 3, apartado 1, de la Decisión Marco 2009/315/JAI y el artículo 3, punto 5, del Reglamento (UE) 2019/816 responderán a las solicitudes de información en el plazo de diez días hábiles a partir de la fecha de recepción de la solicitud de conformidad con el artículo 8, apartado 1, de la Decisión Marco 2009/315/JAI.

([37]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

Artículo 15

Notificación de incidentes

1. Los Estados miembros se asegurarán de que las entidades críticas notifiquen sin demora indebida a la autoridad competente los incidentes que perturben o puedan perturbar de forma significativa la prestación de servicios esenciales. Los Estados miembros se asegurarán de que, salvo que sean incapaces de hacerlo desde el punto de vista operativo, las entidades críticas presenten, en un plazo de veinticuatro horas a partir del momento en que tengan conocimiento de un incidente, una notificación inicial seguida, en su caso, de un informe detallado en el plazo de un mes, a más tardar. A fin de determinar la magnitud de la perturbación, se tendrán en cuenta, en particular, los parámetros siguientes:

a) el número y el porcentaje de usuarios afectados por la perturbación;

b) la duración de la perturbación;

c) la zona geográfica afectada por la perturbación, teniendo en cuenta si la zona está aislada geográficamente.

Cuando un incidente tenga o pueda tener repercusiones significativas en la continuidad de la prestación de servicios esenciales en seis Estados miembros o más, las autoridades competentes de los Estados miembros afectados por el incidente lo notificarán a la Comisión.

2. Las notificaciones a que se refiere el apartado 1, párrafo primero, incluirán toda la información disponible necesaria para que la autoridad competente pueda comprender la naturaleza, la causa y las posibles consecuencias del incidente, incluida cualquier información disponible que sea necesaria para determinar las posibles repercusiones transfronterizas del incidente. Tales notificaciones no acarrearán una mayor responsabilidad para las entidades críticas.

3. Sobre la base de la información facilitada por una entidad crítica en una notificación a que se refiere el apartado 1, la autoridad competente correspondiente, a través del punto de contacto único, informará a los puntos de contacto únicos de los demás Estados miembros afectados en caso de que el incidente tenga o pueda tener repercusiones significativas en las entidades críticas y en la continuidad de la prestación de servicios esenciales para o en uno o varios Estados miembros.

El punto de contacto único que envíe y reciba información con arreglo al párrafo primero tratará dicha información, de conformidad con el Derecho de la Unión o nacional, de forma que se respete su confidencialidad y se protejan la seguridad y los intereses comerciales de la entidad crítica de que se trate.

4. Tan pronto como sea posible tras haber recibido la notificación a que se refiere el apartado 1, la autoridad competente correspondiente facilitará a la entidad crítica afectada información de seguimiento pertinente, incluida la información que pueda respaldar una respuesta eficaz de la entidad crítica al incidente en cuestión. Los Estados miembros informarán al público cuando consideren que sea de interés público hacerlo.

Artículo 16

Normas

A fin de promover una aplicación convergente de la presente Directiva, los Estados miembros, cuando resulte útil y sin imponer ni favorecer el uso de un tipo específico de tecnología, fomentarán la utilización de normas y especificaciones técnicas europeas e internacionales que sean pertinentes para las medidas de seguridad y resiliencia aplicables a las entidades críticas.

CAPÍTULO IV

ENTIDADES CRITICAS DE ESPECIAL IMPORTANCIA EUROPEA

Artículo 17

Identificación de las entidades críticas de especial importancia europea

1. Se considerará que una entidad es una entidad crítica de especial importancia europea cuando:

a) haya sido identificada como entidad crítica de conformidad con el artículo 6, apartado 1;

b) preste los mismos o similares servicios esenciales a o en seis o más Estados miembros, y

c) haya sido notificada de conformidad con el apartado 3 del presente artículo.

2. Los Estados miembros garantizarán que, tras la notificación a que se refiere el artículo 6, apartado 3, la entidad crítica informe a su autoridad competente en caso de que preste servicios esenciales a o en seis o más Estados miembros. En ese caso, los Estados miembros garantizarán que la entidad crítica informe a su autoridad competente de los servicios esenciales que presta a y en tales Estados miembros y de los Estados miembros a o en los que presta tales servicios esenciales. Los Estados miembros comunicarán sin demora indebida a la Comisión la identidad de dichas entidades críticas y la información facilitada con arreglo al presente apartado.

La Comisión consultará a la autoridad competente del Estado miembro que haya identificado a una entidad crítica a que se refiere el párrafo primero, a la autoridad competente de los demás Estados miembros de que se trate y a la entidad crítica en cuestión. Durante dichas consultas, cada Estado miembro informará a la Comisión en caso de considerar esenciales los servicios prestados a dicho Estado miembro por la entidad crítica.

3. Cuando, a partir de las consultas mencionadas en el apartado 2 del presente artículo, la Comisión determine que la entidad crítica en cuestión presta servicios esenciales a o en seis o más Estados miembros, notificará a dicha entidad crítica, a través de su autoridad competente, que se la considera una entidad crítica de especial importancia europea y le informará de las obligaciones que le incumben en virtud del presente capítulo y de la fecha a partir de la cual le serán exigibles. Una vez que la Comisión informe a la autoridad competente de su decisión de considerar que una entidad crítica es una entidad crítica de especial importancia europea, la autoridad competente transmitirá dicha notificación a la entidad crítica sin demora indebida.

4. El presente capítulo se aplicará a la entidad crítica de especial importancia europea de que se trate a partir de la fecha de recepción de la notificación mencionada en el apartado 3 del presente artículo.

Artículo 18

Misiones de asesoramiento

1. A petición del Estado miembro que haya identificado que una entidad crítica de especial importancia europea es una entidad crítica con arreglo al artículo 6, apartado 1, la Comisión organizará una misión de asesoramiento a fin de evaluar las medidas adoptadas por dicha entidad crítica con el fin de cumplir sus obligaciones con arreglo al capítulo III.

2. A iniciativa propia o a petición de uno o más Estados miembros a o en los que se preste el servicio esencial y siempre que cuente con el acuerdo del Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, la Comisión organizará una misión de asesoramiento a tenor del apartado 1 del presente artículo.

3. Previa solicitud motivada de la Comisión o de uno o varios de los Estados miembros a o en los que se preste el servicio esencial, el Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, facilitará a la Comisión la siguiente información:

a) las partes pertinentes de la evaluación de riesgos de la entidad crítica;

b) una lista de las medidas pertinentes tomadas de conformidad con el artículo 13;

c) las medidas de supervisión o ejecución, incluidas las evaluaciones del cumplimiento o las órdenes emitidas, que su autoridad competente haya emprendido con arreglo a los artículos 21 y 22 con respecto a dicha entidad crítica.

4. La misión de asesoramiento informará de sus conclusiones a la Comisión, al Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, a los Estados miembros a o en los que se preste el servicio esencial y a la entidad crítica en cuestión en el plazo de tres meses a partir de la conclusión de la misión de asesoramiento.

Los Estados miembros a o en los que se preste el servicio esencial analizarán el informe mencionado en el párrafo primero y, en caso necesario, informarán a la Comisión sobre el cumplimiento o no por la entidad crítica de especial importancia europea de que se trate de sus obligaciones con arreglo al capítulo III y, si ha lugar, sobre las medidas que podrían adoptarse para aumentar la resiliencia de dicha entidad crítica.

Sobre la base de la información mencionada en el párrafo segundo del presente apartado, la Comisión comunicará al Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, a los Estados miembros a o en los que se preste el servicio esencial y a dicha entidad crítica su dictamen sobre el cumplimiento o no por la entidad crítica de sus obligaciones con arreglo al capítulo III y, si ha lugar, sobre las medidas que podrían adoptarse para aumentar la resiliencia de dicha entidad crítica.

El Estado miembro que haya identificado a una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, se asegurará de que su autoridad competente y la entidad crítica de que se trate tengan debidamente en cuenta el dictamen mencionado en el párrafo tercero del presente apartado e informará a la Comisión y a los Estados miembros a o en los que se preste el servicio esencial de las medidas adoptadas de conformidad con dicho dictamen.

5. Cada misión de asesoramiento estará compuesta por expertos del Estado miembro en el que esté situada la entidad crítica de especial importancia europea, expertos de los Estados miembros a o en los que se preste el servicio esencial y por representantes de la Comisión. Dichos Estados miembros podrán proponer candidatos a formar parte de una misión de asesoramiento. La Comisión, tras consultar al Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1, seleccionará y nombrará a los miembros de cada misión de asesoramiento en función de su capacidad profesional y garantizando, cuando sea posible, una representación geográficamente equilibrada de todos esos Estados miembros. Cuando sea necesario, los miembros de la misión de asesoramiento deberán disponer de una habilitación de seguridad adecuada y en vigor. La Comisión sufragará los gastos relacionados con la participación en la misión de asesoramiento.

La Comisión organizará el programa de cada misión de asesoramiento, en consulta con los miembros de la misión de asesoramiento en cuestión y de acuerdo con el Estado miembro que haya identificado una entidad crítica de especial importancia europea como entidad crítica con arreglo al artículo 6, apartado 1.

6. La Comisión adoptará un acto de ejecución por el que se establezcan normas sobre las disposiciones de procedimiento aplicables a las solicitudes de organización de misiones de asesoramiento, a la tramitación de tales solicitudes, a la realización de las misiones de asesoramiento y la elaboración de sus informes y al tratamiento de la comunicación del dictamen de la Comisión a que se refiere el apartado 4, párrafo tercero, del presente artículo y a las medidas adoptadas, teniendo debidamente en cuenta la confidencialidad y la sensibilidad comercial de la información en cuestión. Dicho acto de ejecución se adoptará de conformidad con el procedimiento de examen a que se refiere el artículo 24, apartado 2.

7. Los Estados miembros se asegurarán de que las entidades críticas de especial importancia europea proporcionen a la misión de asesoramiento acceso a la información, los sistemas y las instalaciones relacionados con la prestación de sus servicios esenciales necesarios para llevar a cabo la misión de asesoramiento de que se trate.

8. Las misiones de asesoramiento se llevarán a cabo de conformidad con el Derecho nacional aplicable del Estado miembro en el que tengan lugar, con respecto a la responsabilidad del Estado miembro en materia de seguridad nacional y la protección de sus intereses de seguridad.

9. Al organizar las misiones de asesoramiento, la Comisión tendrá en cuenta los informes de todas las inspecciones realizadas por la Comisión con arreglo a los Reglamentos (CE) n.º 725/2004 y (CE) n.º 300/2008, así como los informes de cualquier supervisión efectuada por la Comisión en virtud de la Directiva 2005/65/CE en relación con la entidad crítica de que se trate.

10. La Comisión informará al Grupo de Resiliencia de las Entidades Críticas a que se refiere el artículo 19 cada vez que se organice una misión de asesoramiento. Además, el Estado miembro en el que tuvo lugar la misión de asesoramiento y la Comisión informarán al Grupo de Resiliencia de las Entidades Críticas acerca de las conclusiones principales de la misión de asesoramiento y de la experiencia adquirida, con vistas a fomentar el aprendizaje mutuo.

CAPÍTULO V

COOPERACIÓN Y PRESENTACIÓN DE INFORMES

Artículo 19

Grupo de Resiliencia de las Entidades Críticas

1. Se establece un Grupo de Resiliencia de las Entidades Críticas. El Grupo de Resiliencia de las Entidades Críticas apoyará a la Comisión y facilitará la cooperación entre los Estados miembros y el intercambio de información sobre cuestiones relacionadas con la presente Directiva.

2. El Grupo de Resiliencia de las Entidades Críticas estará compuesto por representantes de los Estados miembros y de la Comisión que dispongan de habilitación de seguridad, cuando proceda. Cuando sea pertinente para el desempeño de sus funciones, el Grupo de Resiliencia de las Entidades Críticas podrá invitar a partes interesadas pertinentes a participar en su trabajo. Si así lo solicita el Parlamento Europeo, la Comisión también podrá invitar a expertos del Parlamento Europeo a asistir a las reuniones del Grupo de Resiliencia de las Entidades Críticas.

El representante de la Comisión presidirá el Grupo de Resiliencia de las Entidades Críticas.

3. El Grupo de Resiliencia de las Entidades Críticas desempeñará las siguientes funciones:

a) asistir a la Comisión en la prestación de ayuda a los Estados miembros para que refuercen su capacidad de contribuir a garantizar la resiliencia de las entidades críticas de conformidad con la presente Directiva;

b) analizar las estrategias para determinar las mejores prácticas con respecto a ellas;

c) facilitar el intercambio de mejores prácticas en lo que respecta a la identificación de las entidades críticas por parte de los Estados miembros con arreglo al artículo 6, apartado 1, también en relación con las dependencias transfronterizas e intersectoriales y en lo referente a los riesgos e incidentes;

d) cuando proceda, realizar contribuciones, en torno a cuestiones relacionadas con la presente Directiva, a documentos relativos a la resiliencia a escala de la Unión;

e) contribuir a la preparación de las directrices a que se refieren el artículo 7, apartado 3, y el artículo 13, apartado 5, y, previa solicitud, de cualquier acto delegado o de ejecución adoptado en virtud de la presente Directiva;

f) analizar los informes de síntesis a que se refiere el artículo 9, apartado 3, con vistas a promover el intercambio de mejores prácticas sobre las medidas adoptadas de conformidad con el artículo 15, apartado 3;

g) intercambiar información sobre las mejores prácticas relacionadas con la notificación de incidentes a que se refiere el artículo 15;

h) debatir los informes de síntesis de las misiones de asesoramiento y la experiencia adquirida de conformidad con el artículo 18, apartado 10;

i) intercambiar información sobre las actividades y las mejores prácticas en materia de innovación, investigación y desarrollo en relación con la resiliencia de las entidades críticas de conformidad con la presente Directiva;

j) cuando proceda, intercambiar información sobre cuestiones relativas a la resiliencia de las entidades críticas con las instituciones, órganos y organismos pertinentes de la Unión.

4. A más tardar el 17 de enero de 2025, y posteriormente cada dos años, el Grupo de Resiliencia de las Entidades Críticas establecerá un programa de trabajo en el que exponga las acciones que deban emprenderse para cumplir sus objetivos y tareas. Dicho programa de trabajo deberá ser coherente con los requisitos y objetivos de la presente Directiva.

5. El Grupo de Resiliencia de las Entidades Críticas se reunirá periódicamente, y como mínimo una vez al año, con el Grupo de Cooperación establecido en virtud de la Directiva (UE) 2022/2555 a fin de fomentar y facilitar la cooperación y el intercambio de información.

6. La Comisión podrá adoptar actos de ejecución que establezcan las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de Resiliencia de las Entidades Críticas, de conformidad con el artículo 1, apartado 4. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 24, apartado 2.

7. La Comisión presentará al Grupo de Resiliencia de las Entidades Críticas un informe de síntesis de la información facilitada por los Estados miembros de conformidad con el artículo 4, apartado 3, y el artículo 5, apartado 4, a más tardar el 17 de enero de 2027, y posteriormente siempre que sea necesario y como mínimo cada cuatro años.

Artículo 20

Apoyo de la Comisión a las autoridades competentes y a las entidades críticas

1. La Comisión apoyará, cuando proceda, a los Estados miembros y a las entidades críticas en el cumplimiento de sus obligaciones en virtud de la presente Directiva. La Comisión elaborará una visión de conjunto a escala de la Unión de los riesgos transfronterizos e intersectoriales para la prestación de servicios esenciales, organizará las misiones de asesoramiento a que se refieren el artículo 13, apartado 4, y el artículo 18, y facilitará el intercambio de información entre Estados miembros y expertos en toda la Unión.

2. La Comisión complementará las actividades de los Estados miembros a que se refiere el artículo 10 mediante el desarrollo de mejores prácticas, materiales y metodologías de orientación, y actividades y ejercicios de formación transfronterizos para poner a prueba la resiliencia de las entidades críticas.

3. La Comisión informará a los Estados miembros sobre los recursos financieros a escala de la Unión puestos a disposición de los Estados miembros para aumentar la resiliencia de las entidades críticas.

CAPÍTULO VI

SUPERVISIÓN Y EJECUCIÓN

Artículo 21

Supervisión y ejecución

1. A fin de evaluar el cumplimiento de las obligaciones establecidas en la presente Directiva por parte de las entidades identificadas por los Estados miembros como entidades críticas con arreglo al artículo 6, apartado 1, los Estados miembros garantizarán que las autoridades competentes dispongan de las facultades y medios necesarios para:

a) realizar inspecciones *in situ* de las infraestructuras críticas y de las instalaciones que utilice la entidad crítica para prestar sus servicios esenciales y actividades de supervisión externa de las medidas adoptadas por las entidades críticas con arreglo al artículo 13;

b) realizar u ordenar auditorías con respecto a entidades críticas.

2. Los Estados miembros garantizarán que las autoridades competentes dispongan de las facultades y medios necesarios para exigir, cuando sea necesario para el desempeño de sus funciones con arreglo a la presente Directiva, que las entidades con arreglo a la Directiva (UE) 2022/2555 que los Estados miembros hayan identificado como entidades críticas con arreglo a la presente Directiva faciliten, en un plazo razonable fijado por dichas autoridades:

a) la información necesaria para evaluar si las medidas adoptadas por las citadas entidades para garantizar su resiliencia cumplen los requisitos establecidos en el artículo 13;

b) pruebas de la aplicación efectiva de dichas medidas, incluidos los resultados de una auditoría realizada por un auditor cualificado e independiente seleccionado por la entidad y a expensas de esta.

Cuando exijan dicha información, las autoridades competentes indicarán con qué objeto la piden y especificarán la información requerida.

3. Sin perjuicio de la posibilidad de imponer sanciones de conformidad con el artículo 22, las autoridades competentes, tras las medidas de supervisión a que se refiere el apartado 1 del presente artículo o la evaluación de la información a que se refiere su apartado 2, podrán requerir a las entidades críticas correspondientes que adopten las medidas necesarias y proporcionadas para subsanar cualquier incumplimiento detectado de la presente Directiva, en un plazo razonable fijado por tales autoridades, y que les faciliten información sobre las medidas adoptadas. Dichos requerimientos tendrán en cuenta, en particular, la gravedad del incumplimiento.

4. Los Estados miembros garantizarán que las facultades establecidas en los apartados 1, 2 y 3 únicamente puedan ejercerse con las salvaguardias adecuadas. Dichas salvaguardias garantizarán, en particular, que dichas facultades se ejerzan de manera objetiva, transparente y proporcionada, y que los derechos e intereses legítimos de las entidades críticas interesadas, como la protección de los secretos comerciales y empresariales, estén debidamente protegidos, incluidos su derecho a ser oídas y su derecho de defensa y de tutela judicial efectiva ante un órgano jurisdiccional independiente.

5. Los Estados miembros garantizarán que, cuando una autoridad competente con arreglo a la presente Directiva evalúe el cumplimiento de las obligaciones de una entidad crítica con arreglo al presente artículo, dicha autoridad competente informe a las autoridades competentes de los Estados miembros de que se trate con arreglo a la Directiva (UE) 2022/2555. A tal fin, los Estados miembros garantizarán que las autoridades competentes con arreglo a la presente Directiva puedan solicitar a las autoridades competentes con arreglo a la Directiva (UE) 2022/2555 que ejerzan sus facultades de supervisión y ejecución en relación con una entidad con arreglo a dicha Directiva que haya sido identificada como entidad crítica con arreglo a la presente Directiva. A tal efecto, los Estados miembros garantizarán que las autoridades competentes con arreglo a la presente Directiva cooperen e intercambien información con las autoridades competentes con arreglo a la Directiva (UE) 2022/2555.

Artículo 22

Sanciones

Los Estados establecerán el régimen de sanciones aplicables a cualquier incumplimiento de las medidas 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 octubre de 2024, y le notificarán sin demora toda modificación posterior.

CAPÍTULO VII

ACTOS DELEGADOS Y ACTOS DE EJECUCION

Artículo 23

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 5, apartado 1, se otorgan a la Comisión por un período de dos años a partir del 16 de enero de 2023.

3. La delegación de poderes mencionada en el artículo 5, apartado 1, 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 5, apartado 1, 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 24

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.

CAPÍTULO VIII

DISPOSICIONES FINALES

Artículo 25

Presentación de informes y revisión

A más tardar el 17 de julio de 2027, la Comisión presentará un informe al Parlamento Europeo y al Consejo en el que se evalúe en qué medida cada Estado miembro ha adoptado las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Directiva.

La Comisión revisará periódicamente el funcionamiento de la presente Directiva e informará al Parlamento Europeo y al Consejo. En dicho informe se evaluará, en particular, el valor añadido de la presente Directiva, su impacto a la hora de garantizar la resiliencia de las entidades críticas y la conveniencia de modificar el anexo de la presente Directiva. La Comisión presentará el primer informe a más tardar el 17 de junio de 2029. A efectos de la presentación de informes con arreglo al presente artículo, la Comisión tendrá en cuenta los documentos pertinentes del Grupo de Resiliencia de las Entidades Críticas.

Artículo 26

Transposición

1. Los Estados miembros adoptarán y publicarán a más tardar el 17 de octubre de 2024 las disposiciones necesarias para dar cumplimiento a lo establecido en la presente Directiva. Informarán de ello inmediatamente a la Comisión.

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 27

Derogación de la Directiva 2008/114/CE

Queda derogada la Directiva 2008/114/CE con efecto a partir del 18 de octubre de 2024.

Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva.

Artículo 28

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 29

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

SECTORES, SUBSECTORES Y CATEGORÍAS DE ENTIDADES

Sectores	Subsectores	Categorías de entidades
1. Energía	a) Electricidad	— Las 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 desempeñan la función de «suministro» tal como se definen en el artículo 2, punto 12, de dicha Directiva.
		— Los gestores de la red de distribución tal como se definen en el artículo 2, punto 29, de la Directiva (UE) 2019/944
		— Los gestores de la red de transporte tal como se definen en el artículo 2, punto 35, de la Directiva (UE) 2019/944
		— Los productores tal como se definen en el artículo 2, punto 38, de la Directiva (UE) 2019/944
		— Los 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])
		— Los participantes en el mercado tal como se definen en el artículo 2, punto 25, del Reglamento (UE) 2019/943 que presten los servicios de agregación, respuesta de demanda o almacenamiento de energía tal como se definen en el artículo 2, puntos 18, 20 y 59, de la Directiva (UE) 2019/944
	b) Sistemas urbanos de calefacción y de refrigeración	— Los operadores de sistemas urbanos de calefacción o 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	— Los operadores de oleoductos de transporte de crudo
		— Los operadores de producción de crudo, instalaciones de refinado y tratamiento, almacenamiento y transporte
		— Las entidades centrales de almacenamiento de crudo tal como se definen en el artículo 2, letra f), de la Directiva 2009/119/CE del Consejo ([4])

Sectores	Subsectores	Categorías de entidades
	d) Gas	— Las empresas suministradoras tal como se definen en el artículo 2, punto 8, de la Directiva 2009/73/CE del Parlamento Europeo y del Consejo ([5])
		— Los gestores de la red de distribución tal como se definen en el artículo 2, punto 6, de la Directiva 2009/73/CE
		— Los gestores de la red de transporte tal como se definen en el artículo 2, punto 4, de la Directiva 2009/73/CE
		— Los gestores de almacenamientos tal como se definen en el artículo 2, punto 10, de la Directiva 2009/73/CE
		— Los gestores de la red de GNL tal como se definen en el artículo 2, punto 12, de la Directiva 2009/73/CE
		— Las compañías de gas natural tal como se definen en el artículo 2, punto 1, de la Directiva 2009/73/CE
		— Los gestores de las instalaciones de refinado y tratamiento de gas natural
	e) Hidrógeno	— Los operadores de producción, almacenamiento y transporte de hidrógeno
2. Transporte	a) Transporte aéreo	— Las compañías aéreas tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008 utilizadas con fines comerciales
		— Las 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]), los aeropuertos tal como se definen en el artículo 2, punto 1, de dicha Directiva, incluidos 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 las entidades que explotan instalaciones anexas dentro de los recintos de los aeropuertos
		— Los operadores de control de la gestión del tránsito que prestan los 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])

Sectores	Subsectores	Categorías de entidades
	b) Transporte por ferrocarril	— Los 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])
		— Las empresas ferroviarias tal como se definen en el artículo 3, punto 1, de la Directiva 2012/34/UE, y los explotadores de las instalaciones de servicio tal como se definen en el artículo 3, punto 12, de dicha Directiva
	c) Transporte marítimo y fluvial	— Las compañías de transporte terrestre, marítimo y costero de pasaje y carga a las que se hace referencia, tal como se definen en el transporte marítimo a tenor del anexo I del Reglamento (CE) n.º 725/2004, con exclusión de los buques explotados por dichas compañías
		— Los organismos gestores de los puertos tal como se definen en el artículo 3, punto 1, de la Directiva 2005/65/CE, incluidas las instalaciones portuarias de estos tal como se definen en el artículo 2, punto 11, del Reglamento (CE) n.º 725/2004, y las entidades que explotan obras y equipos en los puertos
		— Los operadores de los 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 ([10])
	d) Transporte por carretera	— Las autoridades viarias tal como se definen en el artículo 2, punto 12, del Reglamento Delegado (UE) 2015/962 de la Comisión ([11]) 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 es una parte no esencial de su actividad general
		— Los 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 ([12])
	e) Transporte público	— Los operadores de servicio público tal como se definen en el artículo 2, letra d), del Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo ([13])
3. Banca		— Las entidades de crédito tal como se definen en el artículo 4, punto 1, del Reglamento (UE) n.º 575/2013
4. Infraestructuras de los mercados financieros		— Los gestores de los centros de negociación tal como se definen en el artículo 4, punto 24, de la Directiva 2014/65/UE
		— Las entidades de contrapartida central (ECC) tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 648/2012

Sectores	Subsectores	Categorías de entidades
5. Sanidad		— Los 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 ([14])
		— Los laboratorios de referencia de la UE a que se refiere el artículo 15 del Reglamento (UE) 2022/2371 del Parlamento Europeo y del Consejo ([15])
		— Las entidades que realizan actividades de investigación y desarrollo sobre los medicamentos tal como se definen en el artículo 1, punto 2, de la Directiva 2001/83/CE del Parlamento Europeo y del Consejo ([16])
		— Las entidades que fabrican productos farmacéuticos de base y especialidades farmacéuticas a que se refiere la sección C, división 21, de la NACE Rev. 2
		— Las entidades que fabrican productos sanitarios que se consideran indispensables durante una emergencia de salud pública (incluidos en «la 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 ([17])
		— Las entidades con autorización de distribución a que se refiere el artículo 79 de la Directiva 2001/83/CE
6. Agua potable		— Los 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 ([18]), excluidos los distribuidores para los cuales la distribución de aguas destinadas al consumo humano solo es una parte no esencial de su actividad general de distribución de otros bienes y productos básicos
7. Aguas residuales		— Las empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, aguas residuales domésticas o aguas residuales industriales tal como se definen en el artículo 2, puntos 1, 2 y 3, de la Directiva 91/271/CEE del Consejo ([19]), excluidas las empresas para las cuales la recogida, la eliminación o el tratamiento de aguas residuales urbanas, aguas residuales domésticas o aguas residuales industriales es una parte no esencial de su actividad general

Sectores	Subsectores	Categorías de entidades
8. Infraestructura digital		— Los proveedores de puntos de intercambio de internet tal como se definen en el artículo 6, punto 18, de la Directiva (UE) 2022/2555
		— Los proveedores de servicios de DNS tal como se definen en el artículo 6, punto 20, de la Directiva (UE) 2022/2555, excluidos los operadores de servidores raíz
		— Los registros de nombres de dominio de primer nivel tal como se definen en el artículo 6, punto 21, de la Directiva (UE) 2022/2555
		— Los proveedores de servicios de computación en nube tal como se definen en el artículo 6, punto 30, de la Directiva (UE) 2022/2555
		— Los proveedores de servicios de centro de datos tal como se definen en el artículo 6, punto 31, de la Directiva (UE) 2022/2555
		— Los proveedores de redes de distribución de contenidos tal como se definen en el artículo 6, punto 32, de la Directiva (UE) 2022/2555
		— Los prestadores de servicios de confianza tal como se definen en el artículo 3, punto 19, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([20])
		— Los proveedores de redes públicas de comunicaciones electrónicas tal como se definen en el artículo 2, punto 8, de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo ([21])
		— Los proveedores de servicios de comunicaciones electrónicas tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2018/1972, en la medida en que sus servicios estén a disposición del público
9. Administración pública		— Las entidades de la administración pública de las administraciones centrales, definidas por los Estados miembros de conformidad el Derecho nacional
10. Espacio		— Los operadores de infraestructuras terrestres, cuya propiedad, gestión y explotación corresponde a Estados miembros o entidades privadas, que apoyan la prestación de servicios espaciales, excluidos los proveedores de redes públicas de comunicaciones electrónicas tal como se definen en el artículo 2, punto 8, de la Directiva (UE) 2018/1972

Sectores	Subsectores	Categorías de entidades
11. Producción, transformación y distribución de alimentos		— Las 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 ([22]) que se dedican exclusivamente a la logística y a la distribución al por mayor y a la producción y transformación industrial a gran escala

([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]) 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).

([11]) 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).

([12]) 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).

([13]) Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo, de 23 de octubre de 2007, sobre los servicios públicos de transporte de viajeros por ferrocarril y carretera y por el que se derogan los Reglamentos (CEE) n.º 1191/69 y (CEE) n.º 1107/70 del Consejo (DO L 315 de 3.12.2007, p. 1).

([14]) 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).

([15]) 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).

([16]) 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).

([17]) 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).

([18]) 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).

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

([20]) 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).

([21]) 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).

([22]) 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).

ISSN 1977-0685 (edición electrónica)
ISSN 1725-2512 (edición papel)

Oficina de Publicaciones
de la Unión Europea
L-2985 Luxemburgo
LUXEMBURGO

ES