BASE DE DATOS DE Norma CEF.-
Referencia: NCL013120

REGLAMENTO (UE) 2022/2554, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 14 de diciembre, 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.

(DOUE L 333, de 27 de diciembre de 2022)

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
Visto el dictamen del Comité Económico y Social Europeo
De conformidad con el procedimiento legislativo ordinario

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 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 000entidades 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 2018titulada «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 (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 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 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 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.

(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 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. 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.

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 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 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.

(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. 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.

(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 (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 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, 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, y los fondos de pensiones de empleo que 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, 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 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.º1024/2013 del Consejo 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.

(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. 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 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.

(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 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.º1024/2013, 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 2016sobre la mejora de la legislación. 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.

(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, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014 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, 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, 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.

(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, emitió su dictamen el 10 de mayo de 2021.

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.

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, 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) «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;

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;

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;

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.º1060/2009;

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;

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;

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.º1094/2010 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.

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 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.

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.º1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º1095/2010.

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.º1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º1095/2010.

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.º1093/2010, (UE) n.º1094/2010 o (UE) n.º1095/2010, 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.º1093/2010, el artículo 57, apartado 1, del Reglamento (UE) n.º1094/2010 y el artículo 57, apartado 1, del Reglamento (UE) n.º1095/2010, 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.º1093/2010, el artículo 56, apartado 1, del Reglamento (UE) n.º1094/2010 y el artículo 56, apartado 1, del Reglamento (UE) n.º1095/2010.

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.º1093/2010, el artículo 16 del Reglamento (UE) n.º1094/2010 y el artículo 16 del Reglamento (UE) n.º1095/2010, 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.º1093/2010, los artículos 60 y 61 del Reglamento (UE) n.º1094/2010 y los artículos 60 y 61 del Reglamento (UE) n.º1095/2010.

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.º1093/2010, (UE) n.º1094/2010 y (UE) n.º1095/2010, 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.º1093/2010, (UE) n.º1094/2010 y (UE) n.º1095/2010, 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.º1093/2010, los artículos 10 a 14 del Reglamento (UE) n.º1094/2010 y los artículos 10 a 14 del Reglamento (UE) n.º1095/2010.

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.º1093/2010, el artículo 33 del Reglamento (UE) n.º1095/2010 y el artículo 33 del Reglamento (UE) n.º1094/2010, 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.º1024/2013, 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;

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.º909/2014;

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.º648/2012;

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.º600/2014;

h) en lo que respecta a los registros de operaciones, la autoridad competente designada de conformidad con el artículo 22 del Reglamento (UE) n.º648/2012;

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.º1060/2009;

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;

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.º806/2014, 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 2016sobre 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.

SECCIÓN II. MODIFICACIONES

Artículo 59. *Modificaciones del Reglamento (CE) n.º1060/2009.*

El Reglamento (CE) n.º1060/2009 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.»

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.º648/2012.*

El Reglamento (UE) n.º648/2012 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.»

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.º909/2014 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.»

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.º600/2014.*

El Reglamento (UE) n.º600/2014 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. »

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.»

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
La Presidenta
R. METSOLA

Por el Consejo
El Presidente
M. BEK