2024/1774

25.6.2024

REGLAMENTO DELEGADO (UE) 2024/1774 DE LA COMISIÓN

de 13 de marzo de 2024

por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación que especifican las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC y el marco simplificado de gestión del riesgo relacionado con las TIC

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 ([1]), y en particular su artículo 15, párrafo cuarto, y su artículo 16, apartado 3, párrafo cuarto,

Considerando lo siguiente:

(1) El Reglamento (UE) 2022/2554 abarca una amplia variedad de entidades financieras que difieren en cuanto a su tamaño, estructura y organización interna, así como en cuanto a la naturaleza y complejidad de sus actividades, y que, por lo tanto, presentan más o menos elementos de complejidad o mayores o menores riesgos. Para garantizar que esa variedad se tenga debidamente en cuenta, los requisitos relativos a las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las tecnologías de la información y las comunicaciones (TIC) y los relativos al marco simplificado de gestión del riesgo relacionado con las TIC deben ser proporcionados al tamaño, la estructura, la organización interna, la naturaleza y la complejidad de dichas entidades financieras, así como a los riesgos correspondientes.

(2) Por la misma razón, las entidades financieras sujetas al Reglamento (UE) 2022/2554 deben disponer de cierta flexibilidad en la forma de cumplir los requisitos relativos a las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC y los relativos al marco simplificado de gestión del riesgo relacionado con las TIC. Por tanto, debe permitirse a las entidades financieras utilizar la documentación de la que ya dispongan para cumplir las obligaciones de documentación que se deriven de dichos requisitos. Así pues, solo debe exigirse la elaboración, documentación y aplicación de políticas específicas en materia de seguridad de las TIC respecto de determinados elementos esenciales, teniendo en cuenta, entre otras cosas, las prácticas y normas punteras del sector. Además, es necesario elaborar, documentar y aplicar procedimientos de seguridad de las TIC para cubrir aspectos específicos de la ejecución técnica, en particular la gestión de la capacidad y el rendimiento, la gestión de vulnerabilidades y de parches, la seguridad de los datos y sistemas y el registro.

(3) A fin de garantizar la correcta aplicación a lo largo del tiempo de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el título II, capítulo I, del presente Reglamento, es importante que las entidades financieras asignen correctamente y mantengan todas las funciones y responsabilidades pertinentes relacionadas con la seguridad de las TIC y que establezcan las consecuencias del incumplimiento de las políticas o procedimientos en materia de seguridad de las TIC.

(4) A fin de limitar el riesgo de conflictos de intereses, las entidades financieras deben garantizar la separación de tareas a la hora de asignar funciones y responsabilidades en relación con las TIC.

(5) En interés de la flexibilidad y a fin de simplificar el marco de control de las entidades financieras, estas no deben tener la obligación de elaborar disposiciones específicas sobre las consecuencias del incumplimiento de las políticas, procedimientos y protocolos en materia de seguridad de las TIC a que se refiere el título II, capítulo I, del presente Reglamento cuando tales disposiciones ya estén establecidas en otra política o procedimiento.

([1]) DO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) En un entorno dinámico en el que los riesgos relacionados con las TIC se encuentran en constante evolución, es importante que las entidades financieras elaboren su conjunto de políticas en materia de seguridad de las TIC sobre la base de las prácticas punteras y, cuando proceda, las normas definidas en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([2]). De esta forma, cabe esperar que las entidades financieras a que se refiere el título II del presente Reglamento se mantengan informadas y preparadas en un panorama cambiante.

(7) A fin de garantizar su resiliencia operativa digital, las entidades financieras a que se refiere el título II del presente Reglamento deben, dentro de sus políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC, elaborar y aplicar una política de gestión de activos de TIC, procedimientos de gestión de la capacidad y el rendimiento, y políticas y procedimientos relacionados con las operaciones de TIC. Tales políticas y procedimientos son necesarios para garantizar el seguimiento de la situación de los activos de TIC a lo largo de su ciclo de vida, de modo que se usen y mantengan de manera eficaz (gestión de activos de TIC). Asimismo, las políticas y procedimientos mencionados deben garantizar que se optimice la explotación de los sistemas de TIC y que el rendimiento de los sistemas y de la capacidad de TIC cumpla los objetivos empresariales y de seguridad de la información establecidos (gestión de la capacidad y del rendimiento). Por último, esas políticas y procedimientos deben garantizar la eficacia y fluidez en la gestión y explotación cotidianas de los sistemas de TIC (operaciones de TIC), minimizando así el riesgo de pérdida de confidencialidad, integridad y disponibilidad de los datos. Por tanto, se trata de políticas y procedimientos necesarios para garantizar la seguridad de las redes, ofrecer salvaguardias adecuadas contra las intrusiones y el uso indebido de los datos, y preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos.

(8) A fin de velar por una gestión adecuada del riesgo relacionado con los sistemas de TIC heredados, las entidades financieras deben registrar y hacer un seguimiento de las fechas límite de los servicios de soporte de terceros para las TIC. En vista de las repercusiones que puede tener la pérdida de confidencialidad, integridad y disponibilidad de los datos, las entidades financieras deben centrarse en aquellos activos o sistemas de TIC que sean esenciales para el funcionamiento de la empresa a la hora de registrar y hacer un seguimiento de dichas fechas límite.

(9) Los controles criptográficos pueden garantizar la disponibilidad, autenticidad, integridad y confidencialidad de los datos. Por tanto, las entidades financieras a que se refiere el título II del presente Reglamento deben determinar y aplicar dichos controles siguiendo un enfoque basado en el riesgo. A tal fin, las entidades financieras deben cifrar los datos de que se trate en reposo, en tránsito o, en caso necesario, en uso, sobre la base de los resultados de un proceso doble, a saber, la clasificación de los datos y una evaluación exhaustiva del riesgo relacionado con las TIC. Dada la complejidad que reviste el cifrado de los datos en uso, las entidades financieras a que se refiere el título II del presente Reglamento solo deben cifrar esos datos cuando los resultados de la evaluación del riesgo relacionado con las TIC así lo aconsejen. No obstante, cuando el cifrado de los datos en uso no sea factible o resulte demasiado complejo, las entidades financieras a que se refiere el título II del presente Reglamento han de poder proteger la confidencialidad, integridad y disponibilidad de los datos de que se trate a través de otras medidas de seguridad de las TIC. Habida cuenta de los rápidos avances tecnológicos en el ámbito de las técnicas criptográficas, las entidades financieras a que se refiere el título II del presente Reglamento deben mantenerse al tanto de los avances pertinentes en materia de criptoanálisis y tener en cuenta las prácticas y normas punteras. Por consiguiente, las entidades financieras a que se refiere el título II del presente Reglamento deben adoptar un enfoque flexible, basado en la mitigación y el seguimiento de los riesgos, para hacer frente al panorama dinámico de las amenazas criptográficas, incluidas las amenazas derivadas de los avances en el ámbito cuántico.

(10) La seguridad de las operaciones de TIC y las políticas, procedimientos, protocolos y herramientas operativos son fundamentales para garantizar la confidencialidad, integridad y disponibilidad de los datos. Un aspecto clave es la estricta separación entre los entornos de producción de TIC y los entornos en los que se desarrollen y prueben los sistemas de TIC u otros entornos distintos del de producción. Dicha separación debe constituir una medida fundamental para la seguridad de las TIC frente a acciones no intencionadas y no autorizadas de acceso a datos, modificación de datos o supresión de datos en el entorno de producción, que podrían provocar graves perturbaciones en las operaciones comerciales de las entidades financieras a que se refiere el título II del presente Reglamento. Ahora bien, teniendo en cuenta las prácticas actuales de desarrollo de sistemas de TIC, las entidades financieras deben estar autorizadas, en circunstancias excepcionales, a realizar pruebas en entornos de producción, siempre que justifiquen esas pruebas y obtengan la aprobación requerida.

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

(11) La rápida evolución del panorama de las TIC, de las vulnerabilidades en materia de TIC y de las ciberamenazas exige un enfoque proactivo y global para determinar, evaluar y hacer frente a tales vulnerabilidades. Sin ese enfoque, las entidades financieras y sus clientes, usuarios o contrapartes pueden verse gravemente expuestos a riesgos, lo que pondría en peligro su resiliencia operativa digital, la seguridad de sus redes y la disponibilidad, autenticidad, integridad y confidencialidad de los datos que las políticas y procedimientos en materia de seguridad de las TIC deben proteger. Por consiguiente, las entidades financieras a que se refiere el título II del presente Reglamento deben determinar y subsanar las vulnerabilidades en su entorno de TIC, y tanto las entidades financieras como sus proveedores terceros de servicios de TIC deben adherirse a un marco de gestión de vulnerabilidades coherente, transparente y responsable. Por la misma razón, las entidades financieras deben hacer un seguimiento de las vulnerabilidades en materia de TIC utilizando recursos fiables y herramientas automatizadas y verificar que los proveedores terceros de servicios de TIC garanticen una actuación rápida ante las vulnerabilidades en los servicios de TIC prestados.

(12) La gestión de parches debe ser una parte fundamental de las políticas y procedimientos en materia de seguridad de las TIC que, a través de la realización de pruebas y la implementación en un entorno controlado, tienen por objeto resolver las vulnerabilidades detectadas y evitar perturbaciones derivadas de la instalación de parches.

(13) Las entidades financieras, a fin de garantizar una comunicación oportuna y transparente de las amenazas para la seguridad que podrían afectarles a ellas y a sus partes interesadas, deben establecer procedimientos para la divulgación responsable de las vulnerabilidades en materia de TIC a los clientes, las contrapartes y el público. Al establecer dichos procedimientos, las entidades financieras deben tener en cuenta distintos factores, como la gravedad de una vulnerabilidad, sus posibles repercusiones para las partes interesadas y la disponibilidad de una solución o de medidas de mitigación.

(14) Con miras a la asignación de derechos de acceso de usuario, las entidades financieras a que se refiere el título II del presente Reglamento deben establecer medidas firmes para verificar la identificación única de las personas y los sistemas que vayan a acceder a su información. No hacerlo expondría a las entidades financieras a posibles situaciones de acceso no autorizado, violaciones de la seguridad de los datos y actividades fraudulentas, poniendo así en peligro la confidencialidad, integridad y disponibilidad de los datos financieros sensibles. Si bien debe permitirse excepcionalmente el uso de cuentas genéricas o compartidas en circunstancias especificadas por las entidades financieras, estas han de garantizar que se asuma en todo momento la responsabilidad por las acciones realizadas con dichas cuentas. Sin esa salvaguardia, los usuarios malintencionados podrían obstaculizar las medidas de investigación y correctoras, dejando así a las entidades financieras expuestas a actividades malintencionadas no detectadas o sanciones por incumplimiento.

(15) A fin de gestionar los rápidos avances en los entornos de TIC, las entidades financieras a que se refiere el título II del presente Reglamento deben aplicar políticas y procedimientos sólidos de gestión de proyectos de TIC que permitan mantener la disponibilidad, autenticidad, integridad y confidencialidad de los datos. Dichas políticas y procedimientos deben determinar, con independencia de la metodología de gestión de proyectos de TIC escogida por la entidad financiera, los elementos necesarios para que esa gestión se realice correctamente, en particular por lo que respecta a la modificación, adquisición, mantenimiento y desarrollo de los sistemas de TIC de la entidad financiera. En el contexto de tales políticas y procedimientos, las entidades financieras deben adoptar prácticas y métodos de prueba que se ajusten a sus necesidades, siguiendo al mismo tiempo un enfoque basado en el riesgo y garantizando el mantenimiento de un entorno de TIC seguro, fiable y resiliente. A fin de garantizar la ejecución segura de un proyecto de TIC, las entidades financieras deben velar por que el personal de un determinado sector de actividad o una determinada función empresarial que se vean influidos o afectados por el proyecto en cuestión pueda proporcionar la información y los conocimientos especializados necesarios. Con vistas a una supervisión eficaz, deben presentarse al órgano de dirección informes sobre los proyectos de TIC, en particular aquellos que afecten a funciones esenciales o importantes, y sobre los riesgos que lleven aparejados. Las entidades financieras han de adaptar la frecuencia y los detalles de las revisiones y los informes sistemáticos y continuos a la importancia y las dimensiones de los proyectos de TIC de que se trate.

(16) Es preciso garantizar que los paquetes de *software* que adquieran y desarrollen las entidades financieras a que se refiere el título II del presente Reglamento se integren de manera efectiva y segura en el entorno de TIC existente, de conformidad con los objetivos empresariales y de seguridad de la información establecidos. Por consiguiente, las entidades financieras deben evaluar exhaustivamente dichos paquetes de *software*. A tal fin, y con miras a detectar vulnerabilidades y posibles deficiencias de seguridad tanto en los paquetes de *software* como en los sistemas de TIC en general, las entidades financieras deben someter a prueba la seguridad de las TIC. Asimismo, para evaluar la integridad del *software* y garantizar que su uso no plantee riesgos relacionados con la seguridad de las TIC, las entidades financieras deben revisar, utilizando métodos de prueba tanto estáticos como dinámicos, los códigos fuente del *software* adquirido, incluido, cuando sea posible, del *software* propietario suministrado por proveedores terceros de servicios de TIC.

(17) Los cambios, con independencia de su escala, conllevan riesgos inherentes, de manera que pueden plantear riesgos significativos de pérdida de confidencialidad, integridad y disponibilidad de los datos y, en consecuencia, provocar graves perturbaciones de la actividad. Para proteger a las entidades financieras frente a posibles vulnerabilidades y debilidades relacionadas con las TIC que las expongan a riesgos significativos, se precisa un riguroso proceso de verificación que permita confirmar que todos los cambios cumplen los requisitos necesarios en materia de seguridad de las TIC. Por consiguiente, las entidades financieras a que se refiere el título II del presente Reglamento deben, como elemento fundamental de sus políticas y procedimientos en materia de seguridad de las TIC, contar con políticas y procedimientos sólidos para la gestión de cambios en las TIC. A fin de asegurar la objetividad y la eficacia del proceso de gestión de cambios en las TIC, evitar conflictos de intereses y garantizar que los cambios en las TIC se evalúen de forma objetiva, es necesario que las funciones responsables de aprobar dichos cambios estén separadas de las funciones que los soliciten e implementen. Para lograr que las transiciones sean eficaces, que los cambios en las TIC se implementen de forma controlada y que las perturbaciones en el funcionamiento de los sistemas de TIC sean mínimas, las entidades financieras deben asignar funciones y responsabilidades claras que garanticen la planificación de los cambios en las TIC, la realización de las pruebas adecuadas en relación con esos cambios y la calidad. Asimismo, para garantizar que los sistemas de TIC sigan funcionando de manera eficaz y dotarse de una red de seguridad, las entidades financieras deben elaborar y aplicar procedimientos alternativos. Las entidades financieras han de determinar claramente esos procedimientos alternativos y asignar responsabilidades con el fin de garantizar una respuesta rápida y eficaz cuando los cambios en las TIC no se implementen de forma correcta.

(18) Con miras a la detección, gestión y notificación de incidentes relacionados con las TIC, las entidades financieras a que se refiere el título II del presente Reglamento deben establecer una política de incidentes relacionados con las TIC que abarque los componentes de un proceso de gestión de tales incidentes. A tal fin, las entidades financieras deben identificar todos los contactos pertinentes dentro y fuera de la organización que puedan facilitar la correcta coordinación y ejecución de las diferentes fases de ese proceso. Para optimizar la detección de incidentes relacionados con las TIC y la respuesta a ellos, así como para definir tendencias en los incidentes, que constituyen una valiosa fuente de información a la hora de determinar y tratar las causas subyacentes y los problemas de manera eficaz, las entidades financieras deben, en particular, analizar en detalle los incidentes relacionados con las TIC que consideren más significativos, entre otras cosas, debido a su reiteración periódica.

(19) A fin de garantizar la detección temprana y eficaz de las actividades anómalas, las entidades financieras a que se refiere el título II del presente Reglamento deben recopilar, someter a seguimiento y analizar las distintas fuentes de información y asignar las funciones y responsabilidades correspondientes. Por lo que se refiere a las fuentes internas de información, si bien los registros constituyen una fuente extremadamente importante, las entidades financieras no deben basarse únicamente en ellos, sino que deben ampliar sus fuentes e incluir la información comunicada por otras funciones internas, ya que esas funciones suelen ser una valiosa fuente de información pertinente. Por la misma razón, las entidades financieras deben analizar y hacer un seguimiento de la información recabada de fuentes externas, en particular la facilitada por los proveedores terceros de TIC sobre los incidentes que afecten a sus sistemas y redes, así como la información procedente de otras fuentes que las entidades financieras consideren pertinentes. En la medida en que dicha información esté constituida por datos personales, es de aplicación la legislación de la Unión en materia de protección de datos. Los datos personales deben limitarse a lo necesario para la detección de incidentes.

(20) A fin de facilitar la detección de incidentes relacionados con las TIC, las entidades financieras deben conservar pruebas de dichos incidentes. Para garantizar, por una parte, que las pruebas se conserven el tiempo suficiente y evitar, por otra parte, una carga normativa excesiva, las entidades financieras han de determinar el período de conservación teniendo en cuenta, entre otras cosas, el carácter esencial de los datos y los requisitos de conservación derivados del Derecho de la Unión.

(21) Con el fin de garantizar que los incidentes relacionados con las TIC se detecten a tiempo, las entidades financieras a que se refiere el título II del presente Reglamento no deben considerar que los criterios determinados para activar la detección de incidentes relacionados con las TIC y las respuestas a ellos son exhaustivos. Además, si bien las entidades financieras han de tener en cuenta cada uno de esos criterios, no es necesario que las circunstancias descritas en ellos se produzcan simultáneamente y ha de tenerse debidamente en cuenta la importancia de los servicios de TIC afectados para activar los procesos de detección de incidentes relacionados con las TIC y respuesta a ellos.

(22) Al elaborar una política de continuidad de la actividad en materia de TIC, las entidades financieras a que se refiere el título II del presente Reglamento deben tener en cuenta los componentes fundamentales de la gestión del riesgo relacionado con las TIC, en particular las estrategias de gestión y comunicación de incidentes relacionados con las TIC, el proceso de gestión de cambios en las TIC y los riesgos asociados a los proveedores terceros de servicios de TIC.

(23) Es necesario establecer el conjunto de escenarios que las entidades financieras a que se refiere el título II del presente Reglamento deben tener en cuenta a efectos tanto de la aplicación de los planes de respuesta y recuperación en materia de TIC como del sometimiento a prueba de los planes de continuidad de la actividad en materia de TIC. Dichos escenarios deben servir de punto de partida para que las entidades financieras analicen tanto la pertinencia y verosimilitud de cada escenario como la necesidad de elaborar escenarios alternativos. Las entidades financieras han de centrarse en aquellos escenarios en los que la inversión en medidas de resiliencia pueda ser más eficaz y eficiente. Mediante las pruebas de las conmutaciones entre la infraestructura primaria de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes, las entidades financieras deben evaluar si esa capacidad, esas copias y esas instalaciones funcionan de manera eficaz durante un período de tiempo suficiente y cerciorarse de que el funcionamiento normal de la infraestructura primaria de TIC se restablezca de conformidad con los objetivos de recuperación.

(24) Es necesario establecer requisitos relativos al riesgo operativo, y, más concretamente, a la gestión de proyectos de TIC y cambios en las TIC y a la gestión de la continuidad de la actividad en materia de TIC, partiendo de los requisitos que ya se aplican a las entidades de contrapartida central, los depositarios centrales de valores y los centros de negociación, en virtud, respectivamente, de los Reglamentos (UE) n.º 648/2012 ([3]), (UE) n.º 600/2014 ([4]) y (UE) n.º 909/2014 ([5]) del Parlamento Europeo y del Consejo.

(25) El artículo 6, apartado 5, del Reglamento (UE) 2022/2554 exige a las entidades financieras que revisen su marco de gestión del riesgo relacionado con las TIC y presenten a su autoridad competente un informe sobre dicha revisión. A fin de que las autoridades competentes puedan tratar fácilmente la información contenida en esos informes y garantizar la transmisión adecuada de tal información, las entidades financieras deben presentar los informes en un formato electrónico que permita realizar búsquedas.

(26) Los requisitos aplicables a las entidades financieras sujetas al marco simplificado de gestión del riesgo relacionado con las TIC a que se refiere el artículo 16 del Reglamento (UE) 2022/2554 deben centrarse en aquellos ámbitos y elementos clave que, a la luz de la escala, el riesgo, el tamaño y la complejidad de tales entidades financieras, sean, como mínimo, necesarios para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de sus datos y servicios. En ese contexto, dichas entidades financieras deben contar con un marco interno de gobernanza y control en el que se establezcan responsabilidades claras para hacer posible un marco eficaz y sólido de gestión de riesgos. Además, con miras a reducir la carga administrativa y operativa, las mencionadas entidades financieras deben elaborar y documentar una sola política, esto es, una política de seguridad de la información, en la que se especifiquen los principios y normas generales necesarios para proteger la confidencialidad, integridad, disponibilidad y autenticidad de sus datos y servicios.

(27) Las disposiciones del presente Reglamento abordan el ámbito del marco de gestión del riesgo relacionado con las TIC detallando los elementos específicos aplicables a las entidades financieras de conformidad con el artículo 15 del Reglamento (UE) 2022/2554 y diseñando el marco simplificado de gestión del riesgo relacionado con las TIC para las entidades financieras contempladas en el artículo 16, apartado 1, del mismo Reglamento. A fin de garantizar la coherencia entre el marco ordinario y el marco simplificado de gestión del riesgo relacionado con las TIC, y teniendo en cuenta que las disposiciones correspondientes a uno y otro deben comenzar a aplicarse al mismo tiempo, conviene incluirlas en un único acto legislativo.

(28) El presente Reglamento se basa en los proyectos de normas técnicas de regulación presentados a la Comisión por la Autoridad Bancaria Europea, la Autoridad Europea de Seguros y Pensiones de Jubilación y la Autoridad Europea de Valores y Mercados (Autoridades Europeas de Supervisión), en consulta con la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

([3]) Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones (DO L 201 de 27.7.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 173 de 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

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

(29) El Comité Mixto de las Autoridades Europeas de Supervisión a que se refieren el artículo 54 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([6]), el artículo 54 del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([7]) y el artículo 54 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([8]) ha llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de regulación en que se basa el presente Reglamento, ha analizado los posibles costes y beneficios de las normas propuestas y ha solicitado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1093/2010, el Grupo de Partes Interesadas del Sector de Seguros y Reaseguros y el Grupo de Partes Interesadas del Sector de Pensiones de Jubilación creados de conformidad con el artículo 37 del Reglamento (UE) n.º 1094/2010, y el Grupo de Partes Interesadas del Sector de los Valores y Mercados creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010.

(30) En la medida en que el cumplimiento de las obligaciones establecidas en el presente acto requiera el tratamiento de datos personales, deben aplicarse plenamente los Reglamentos (UE) 2016/679 ([9]) (UE) 2018/1725 ([10]) del Parlamento Europeo y del Consejo. Por ejemplo, debe respetarse el principio de minimización de datos cuando se recojan datos personales para garantizar la detección adecuada de incidentes. Se ha consultado también al Supervisor Europeo de Protección de Datos acerca del proyecto de texto del presente acto.

HA ADOPTADO EL PRESENTE REGLAMENTO:

TÍTULO I

PRINCIPIO GENERAL

Artículo 1

Perfil de riesgo general y complejidad

Al elaborar y aplicar las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el título II y el marco simplificado de gestión del riesgo relacionado con las TIC a que se refiere el título III, se tendrán en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, la naturaleza y escala de sus servicios, actividades y operaciones, y los elementos que supongan un aumento o una disminución de la complejidad de estos, en particular los elementos relativos a:

a) el cifrado y la criptografía;

b) la seguridad de las operaciones de TIC;

c) la seguridad de las redes;

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

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

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

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

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

d) la gestión de proyectos de TIC y de cambios en las TIC;

e) las posibles repercusiones del riesgo relacionado con las TIC sobre la confidencialidad, integridad y disponibilidad de los datos, y las posibles repercusiones de las perturbaciones sobre la continuidad y disponibilidad de las actividades de la entidad financiera.

TÍTULO II

MAYOR ARMONIZACIÓN DE LAS HERRAMIENTAS, MÉTODOS, PROCESOS Y POLÍTICAS DE GESTIÓN DEL RIESGO RELACIONADO CON LAS TIC DE CONFORMIDAD CON EL ARTÍCULO 15 DEL REGLAMENTO (UE) 2022/2554

CAPÍTULO I

Políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC

Sección 1

Artículo 2

Elementos generales de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC

1. Las entidades financieras velarán por que sus políticas en materia de seguridad de las TIC, la seguridad de la información y los procedimientos, protocolos y herramientas conexos a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554 estén integrados en su marco de gestión del riesgo relacionado con las TIC. Las entidades financieras establecerán políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC, conforme a lo dispuesto en el presente capítulo, que:

a) garanticen la seguridad de las redes;

b) contengan salvaguardias adecuadas contra las intrusiones y el uso indebido de los datos;

c) preserven la disponibilidad, autenticidad, integridad y confidencialidad de los datos, en particular mediante el uso de técnicas criptográficas;

d) garanticen una transmisión exacta y rápida de los datos sin perturbaciones importantes ni demoras indebidas.

2. Las entidades financieras velarán por que las políticas en materia de seguridad de las TIC a que se refiere el apartado 1:

a) estén en consonancia con los objetivos de seguridad de la información contenidos en la estrategia de resiliencia operativa digital a que se refiere el artículo 6, apartado 8, del Reglamento (UE) 2022/2554;

b) indiquen la fecha de su aprobación formal por el órgano de dirección;

c) contengan indicadores y parámetros de medición para:

   i) realizar el seguimiento de la aplicación de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC,

   ii) registrar las excepciones a dicha aplicación,

   iii) garantizar que se mantenga la resiliencia operativa digital de la entidad financiera cuando se produzcan las excepciones a que se refiere el inciso ii);

d) especifiquen las responsabilidades del personal a todos los niveles para garantizar la seguridad de las TIC en la entidad financiera;

e) especifiquen las consecuencias de su incumplimiento por parte del personal de la entidad financiera, cuando las disposiciones a tal efecto no estén establecidas en otras políticas de la entidad financiera;

f) enumeren la documentación que debe conservarse;

g) especifiquen las disposiciones sobre separación de funciones en el contexto del modelo de las tres líneas de defensa u otro modelo interno de gestión y control de riesgos, según proceda, con el fin de evitar los conflictos de intereses;

h) tengan en cuenta las prácticas punteras y, en su caso, las normas definidas en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012;

i) determinen las funciones y responsabilidades a efectos de su propia elaboración, aplicación y mantenimiento, así como de la elaboración, aplicación y mantenimiento de los procedimientos, protocolos y herramientas conexos;

j) se revisen de conformidad con el artículo 6, apartado 5, del Reglamento (UE) 2022/2554;

k) tomen en consideración los cambios importantes que afecten a la entidad financiera, en particular los cambios importantes en sus actividades o procesos, en el panorama de ciberamenazas o en las obligaciones jurídicas aplicables.

Sección 2

Artículo 3

Gestión del riesgo relacionado con las TIC

Las entidades financieras elaborarán, documentarán y aplicarán políticas y procedimientos para la gestión del riesgo relacionado con las TIC que contengan todos los elementos siguientes:

a) la indicación de la aprobación del nivel de tolerancia al riesgo relacionado con las TIC que se haya establecido de conformidad con el artículo 6, apartado 8, letra b), del Reglamento (UE) 2022/2554;

b) un procedimiento y una metodología para llevar a cabo la evaluación del riesgo relacionado con las TIC que determinen:

   i) las vulnerabilidades y amenazas que afecten o puedan afectar a las funciones empresariales sustentadas y a los sistemas de TIC y activos de TIC que sustenten dichas funciones,

   ii) los indicadores cuantitativos o cualitativos para medir las repercusiones y la probabilidad de las vulnerabilidades y amenazas a que se refiere el inciso i);

c) el procedimiento para determinar, aplicar y documentar las medidas de tratamiento de los riesgos relacionados con las TIC que hayan sido detectados y evaluados, incluidas las medidas de tratamiento necesarias para situar el riesgo relacionado con las TIC dentro del nivel de tolerancia al riesgo a que se refiere la letra a);

d) respecto de los riesgos residuales relacionados con las TIC que persistan tras aplicar las medidas de tratamiento a que se refiere la letra c):

   i) disposiciones sobre la determinación de dichos riesgos residuales relacionados con las TIC,

   ii) la asignación de funciones y responsabilidades en relación con:

      1) la aceptación de los riesgos residuales relacionados con las TIC que superen el nivel de tolerancia al riesgo de la entidad financiera a que se refiere la letra a);

      2) el proceso de revisión a que se refiere el inciso iv) de la presente letra d),

   iii) la elaboración de un inventario de los riesgos residuales relacionados con las TIC aceptados, que incluya la justificación para tal aceptación,

   iv) disposiciones sobre la revisión, al menos una vez al año, de los riesgos residuales relacionados con las TIC aceptados, incluido lo siguiente:

      1) determinación de posibles cambios en los riesgos residuales relacionados con las TIC;

      2) evaluación de las medidas de mitigación disponibles;

      3) evaluación de la validez y aplicabilidad, en la fecha de la revisión, de las razones que hayan justificado la aceptación de los riesgos residuales relacionados con las TIC;

e) disposiciones sobre el seguimiento de:

   i) los cambios en el panorama de los riesgos relacionados con las TIC y las ciberamenazas,

   ii) las vulnerabilidades y amenazas internas y externas,

   iii) los riesgos relacionados con las TIC de la entidad financiera, de manera que se detecte rápidamente todo cambio que pueda afectar a su perfil de riesgo relacionado con las TIC;

f) disposiciones sobre un proceso para garantizar que se tenga en cuenta todo cambio en la estrategia empresarial y la estrategia de resiliencia operativa digital de la entidad financiera.

A efectos del párrafo primero, letra c), el procedimiento a que se refiere dicha letra garantizará que:

a) se haga un seguimiento de la eficacia de las medidas aplicadas para el tratamiento del riesgo relacionado con las TIC;

b) se evalúe si se han alcanzado los niveles de tolerancia al riesgo establecidos por la entidad financiera;

c) se evalúe si la entidad financiera ha emprendido acciones para corregir o mejorar dichas medidas en caso necesario.

Sección 3

Gestión de activos de TIC

Artículo 4

Política de gestión de activos de TIC

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán una política de gestión de activos de TIC.

2. La política de gestión de activos de TIC a que se refiere el apartado 1:

a) exigirá el seguimiento y la gestión del ciclo de vida de los activos de TIC que hayan sido identificados y clasificados de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554;

b) exigirá que la entidad financiera lleve un registro de todos los aspectos siguientes:

   i) el identificador único de cada activo de TIC,

   ii) la ubicación, física o lógica, de todos los activos de TIC,

   iii) la clasificación de todos los activos de TIC a que se refiere el artículo 8, apartado 1, del Reglamento (UE) 2022/2254,

   iv) la identidad de los propietarios de los activos de TIC,

   v) las funciones o servicios empresariales sustentados por el activo de TIC de que se trate,

   vi) los requisitos relativos a la continuidad de la actividad en materia de TIC, incluidos los objetivos de tiempo de recuperación y de punto de recuperación,

   vii) si el activo de TIC de que se trate puede estar o está expuesto a redes externas, incluida internet,

   viii) los vínculos e interdependencias entre los activos de TIC y las funciones empresariales que utilicen cada activo de TIC,

   ix) cuando proceda, en relación con todos los activos de TIC, la fecha de finalización de los servicios de soporte normales, ampliados y personalizados del proveedor tercero de servicios de TIC tras la cual los activos de TIC dejarán de contar con el soporte de su suministrador o de un proveedor tercero de servicios de TIC;

c) en el caso de las entidades financieras que no sean microempresas, exigirá que tales entidades conserven la información necesaria para realizar la evaluación específica del riesgo relacionado con las TIC en todos los sistemas de TIC heredados a que se refiere el artículo 8, apartado 7, del Reglamento (UE) 2022/2554.

Artículo 5

Procedimiento de gestión de activos de TIC

1. Las entidades financieras elaborarán, documentarán y aplicarán un procedimiento de gestión de activos de TIC.

2. El procedimiento de gestión de activos de TIC a que se refiere el apartado 1 especificará los criterios para la evaluación del carácter esencial de los activos de información y los activos de TIC que sustenten funciones empresariales. Dicha evaluación tendrá en cuenta lo siguiente:

a) el riesgo relacionado con las TIC que llevan asociado tales funciones empresariales, así como su dependencia de los activos de información o activos de TIC;

b) la forma en que la pérdida de confidencialidad, integridad y disponibilidad de tales activos de información y activos de TIC afectaría a los procesos empresariales y las actividades de las entidades financieras.

Sección 4

Cifrado y criptografía

Artículo 6

Cifrado y controles criptográficos

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán una política de cifrado y controles criptográficos.

2. Las entidades financieras diseñarán la política de cifrado y controles criptográficos a que se refiere el apartado 1 basándose en los resultados de una clasificación de datos aprobada y una evaluación del riesgo relacionado con las TIC. Dicha política contendrá normas sobre todos los aspectos siguientes:

a) el cifrado de los datos en reposo y en tránsito;

b) el cifrado de los datos en uso, cuando proceda;

c) el cifrado de las conexiones de red internas y del tráfico con partes externas;

d) la gestión de claves criptográficas a que se refiere el artículo 7, con normas sobre el uso correcto, la protección y el ciclo de vida de esas claves.

A efectos de la letra b), cuando el cifrado de los datos en uso no sea posible, las entidades financieras tratarán tales datos en un entorno separado y protegido, o adoptarán medidas equivalentes para garantizar la confidencialidad, integridad, autenticidad y disponibilidad de los datos.

3. Las entidades financieras incluirán en la política de cifrado y controles criptográficos a que se refiere el apartado 1 criterios para la selección de técnicas y prácticas de uso en materia de criptografía, tomando en consideración las prácticas punteras y las normas definidas en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012, así como la clasificación de los activos de TIC pertinentes establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554. Las entidades financieras que no puedan adherirse a dichas prácticas punteras o normas, o utilizar las técnicas más fiables, adoptarán medidas de mitigación y de seguimiento que garanticen la resiliencia frente a las ciberamenazas.

4. Las entidades financieras incluirán en la política de cifrado y controles criptográficos a que se refiere el apartado 1 disposiciones para actualizar o modificar, en caso necesario, la tecnología criptográfica, a la luz de la evolución del criptoanálisis. Dichas actualizaciones o modificaciones garantizarán que se preserve la resiliencia de la tecnología criptográfica frente a las ciberamenazas, tal como se exige en el artículo 10, apartado 2, letra a). Las entidades financieras que no puedan actualizar o modificar la tecnología criptográfica adoptarán medidas de mitigación y de seguimiento que garanticen la resiliencia frente a las ciberamenazas.

5. Las entidades financieras incluirán en la política de cifrado y controles criptográficos a que se refiere el apartado 1 la obligación de registrar la adopción de medidas de mitigación y de seguimiento con arreglo a los apartados 3 y 4 y de proporcionar una explicación motivada al respecto.

Artículo 7

Gestión de claves criptográficas

1. Las entidades financieras incluirán en la política de gestión de claves criptográficas a que se refiere el artículo 6, apartado 2, letra d), requisitos relativos a la gestión de las claves criptográficas a lo largo de todo su ciclo de vida, en particular por lo que respecta a su generación, renovación, almacenamiento, copia de seguridad, archivo, recuperación, transmisión, retirada, revocación y destrucción.

2. Las entidades financieras determinarán y aplicarán controles para proteger las claves criptográficas a lo largo de todo su ciclo de vida contra la pérdida, el acceso no autorizado, la divulgación y la modificación. Las entidades financieras diseñarán dichos controles basándose en los resultados de la clasificación de datos aprobada y la evaluación del riesgo relacionado con las TIC.

3. Las entidades financieras elaborarán y aplicarán métodos para sustituir las claves criptográficas en caso de pérdida o cuando esas claves se vean comprometidas o resulten dañadas.

4. Las entidades financieras crearán y mantendrán un registro de todos los certificados y dispositivos de almacenamiento de certificados al menos para los activos de TIC que sustenten funciones esenciales o importantes. Las entidades financieras mantendrán actualizado dicho registro.

5. Las entidades financieras velarán por la rápida renovación de los certificados antes de su expiración.

Sección 5

Seguridad de las operaciones de TIC

Artículo 8

Políticas y procedimientos relacionados con las operaciones de TIC

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán políticas y procedimientos de gestión de las operaciones de TIC. Dichas políticas y procedimientos especificarán el modo en que las entidades financieras llevarán a cabo la explotación, el seguimiento, el control y la restauración de sus activos de TIC, así como la documentación de las operaciones de TIC.

2. Las políticas y procedimientos relacionados con las operaciones de TIC a que se refiere el apartado 1 contendrán todos los elementos siguientes:

a) una descripción de los activos de TIC, incluidos todos los requisitos siguientes:

   i) requisitos relativos a la instalación, el mantenimiento, la configuración y la desinstalación con seguridad de un sistema de TIC,

   ii) requisitos relativos a la gestión de los activos de información utilizados por los activos de TIC, en particular su tratamiento y manejo, tanto automatizado como manual,

   iii) requisitos relativos a la identificación de los sistemas de TIC heredados y su control;

b) controles y seguimiento de los sistemas de TIC, incluidos todos los aspectos siguientes:

   i) requisitos relativos a la copia de seguridad y restauración de los sistemas de TIC,

   ii) requisitos de planificación, teniendo en cuenta las interdependencias entre los sistemas de TIC,

   iii) protocolos para la pista de auditoría y la información de registro del sistema,

   iv) requisitos para garantizar que la realización de auditorías internas y otras pruebas cause las mínimas perturbaciones de las operaciones comerciales,

   v) requisitos relativos a la separación entre los entornos de producción de TIC y los de desarrollo y de pruebas y otros entornos distintos del de producción,

   vi) requisitos para llevar a cabo el desarrollo y las pruebas en entornos separados del entorno de producción,

   vii) requisitos para llevar a cabo el desarrollo y las pruebas en entornos de producción;

c) gestión de errores en relación con los sistemas de TIC, incluidos todos los aspectos siguientes:

i) procedimientos y protocolos para la gestión de errores,

ii) contactos para asistencia y traslado a una instancia jerárquica superior, incluidos los contactos externos para asistencia en caso de problemas operativos o técnicos imprevistos,

iii) procedimientos de reinicio, reversión y recuperación de los sistemas de TIC en caso de interrupción de dichos sistemas.

A efectos de la separación a que se refiere la letra b), inciso v), se tendrán en cuenta todos los componentes del entorno, incluidas las cuentas, los datos o las conexiones, tal como se exige en el artículo 13, apartado 1, letra a).

A efectos de la letra b), inciso vii), las políticas y procedimientos a que se refiere el apartado 1 dispondrán que los casos en que se realicen pruebas en un entorno de producción estén claramente definidos y motivados, sean de duración limitada y cuenten con la aprobación de la función pertinente, de conformidad con el artículo 16, apartado 6. Las entidades financieras garantizarán la disponibilidad, confidencialidad, integridad y autenticidad de los sistemas de TIC y los datos de producción durante las actividades de desarrollo y prueba en el entorno de producción.

Artículo 9

Gestión de la capacidad y el rendimiento

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán procedimientos de gestión de la capacidad y el rendimiento a efectos de:

a) la determinación de los requisitos de capacidad de sus sistemas de TIC;

b) la aplicación de la optimización de recursos;

c) los procedimientos de seguimiento para el mantenimiento y la mejora de:

i) la disponibilidad de datos y de los sistemas de TIC,

ii) la eficiencia de los sistemas de TIC,

iii) la prevención de la falta de capacidad en materia de TIC.

2. Los procedimientos de gestión de la capacidad y el rendimiento a que se refiere el apartado 1 garantizarán que las entidades financieras adopten medidas adecuadas para tener en cuenta las especificidades de los sistemas de TIC con procesos de adquisición o aprobación largos o complejos o los sistemas de TIC que requieren un uso intensivo de recursos.

Artículo 10

Gestión de vulnerabilidades y parches

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán procedimientos de gestión de vulnerabilidades.

2. Los procedimientos de gestión de vulnerabilidades a que se refiere el apartado 1 deberán:

a) determinar los recursos de información que sean pertinentes y fiables para desarrollar y mantener la sensibilización sobre las vulnerabilidades, y actualizarlos;

b) garantizar la realización de exploraciones y evaluaciones automatizadas de vulnerabilidad de los activos de TIC cuya frecuencia y alcance serán acordes con la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554 y con el perfil de riesgo general del activo de TIC;

c) verificar:

i) si los proveedores terceros de servicios de TIC gestionan las vulnerabilidades relacionadas con los servicios de TIC prestados a la entidad financiera,

ii) si dichos proveedores de servicios informan a la entidad financiera al menos de las vulnerabilidades graves y de las estadísticas y tendencias de manera oportuna;

d) hacer un seguimiento del uso de:

i) las bibliotecas de terceros, incluidas las bibliotecas de código abierto, a las que recurran los servicios de TIC que sustentan funciones esenciales o importantes,

ii) los servicios de TIC desarrollados por la propia entidad financiera o personalizados o desarrollados específicamente para la entidad financiera por un proveedor tercero de servicios de TIC;

e) establecer procedimientos para la divulgación responsable de las vulnerabilidades a los clientes, las contrapartes y el público;

f) dar prioridad a la implementación de parches y otras medidas de mitigación para hacer frente a las vulnerabilidades detectadas;

g) hacer un seguimiento de la subsanación de las vulnerabilidades y verificar esa subsanación;

h) exigir el registro de toda vulnerabilidad detectada que afecte a los sistemas de TIC y el seguimiento de su resolución.

A efectos de la letra b), las entidades financieras llevarán a cabo las exploraciones y evaluaciones automatizadas de vulnerabilidad al menos semanalmente en el caso de los activos de TIC que sustenten funciones esenciales o importantes.

A efectos de la letra c), las entidades financieras solicitarán a los proveedores terceros de servicios de TIC que investiguen las vulnerabilidades pertinentes, determinen las causas subyacentes y apliquen las medidas de mitigación adecuadas.

A efectos de la letra d), las entidades financieras, en su caso en colaboración con el proveedor tercero de servicios de TIC, harán un seguimiento de la versión y las posibles actualizaciones de las bibliotecas de terceros. En el caso de los activos de TIC o componentes de activos de TIC listos para usar (*off-the-shelf*) que se adquieran y utilicen en la explotación de servicios de TIC que no sustenten funciones esenciales o importantes, las entidades financieras harán, en la medida de lo posible, un seguimiento del uso de bibliotecas de terceros, incluidas las bibliotecas de código abierto.

A efectos de la letra f), las entidades financieras tendrán en cuenta la gravedad de la vulnerabilidad, la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554 y el perfil de riesgo de los activos de TIC afectados por las vulnerabilidades detectadas.

3. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán procedimientos de gestión de parches.

4. Los procedimientos de gestión de parches a que se refiere el apartado 3 deberán:

a) en la medida de lo posible, determinar y evaluar los parches de *software* y *hardware* y las actualizaciones disponibles utilizando herramientas automatizadas;

b) determinar los procedimientos de emergencia para el parcheo y la actualización de los activos de TIC;

c) probar e implementar los parches de *software* y *hardware* y las actualizaciones con arreglo al artículo 8, apartado 2, letra b), incisos v), vi) y vii);

d) fijar plazos para la instalación de parches de *software* y *hardware* y actualizaciones y establecer procedimientos de traslado a la instancia jerárquica superior en caso de que dichos plazos no puedan cumplirse.

Artículo 11

Seguridad de los datos y sistemas

1. Dentro de las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC a que se refiere el artículo 9, apartado 2, del Reglamento (UE) 2022/2554, las entidades financieras elaborarán, documentarán y aplicarán un procedimiento de seguridad de los datos y sistemas.

2. El procedimiento de seguridad de los datos y sistemas a que se refiere el apartado 1 contendrá todos los elementos relacionados con la seguridad de los datos y los sistemas de TIC que se indican a continuación, teniendo en cuenta la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554:

a) las restricciones de acceso a que se refiere el artículo 21 del presente Reglamento, que respaldarán los requisitos de protección de cada nivel de clasificación;

b) la determinación de una configuración segura de referencia para los activos de TIC que minimice su exposición a ciberamenazas y medidas para verificar periódicamente que dicha configuración se aplique de manera efectiva;

c) la determinación de medidas de seguridad para garantizar que únicamente se instale *software* autorizado en los sistemas de TIC y los dispositivos de nodo final;

d) la determinación de medidas de seguridad contra códigos maliciosos;

e) la determinación de medidas de seguridad para garantizar que únicamente se utilicen soportes de almacenamiento de datos, sistemas y dispositivos de nodo final autorizados a la hora de transferir y almacenar datos de la entidad financiera;

f) los siguientes requisitos para garantizar el uso seguro de los dispositivos de nodo final portátiles y los dispositivos de nodo final no portátiles privados:

   i) el requisito de utilizar una solución de gestión para gestionar a distancia los dispositivos de nodo final y borrar a distancia los datos de la entidad financiera,

   ii) el requisito de utilizar mecanismos de seguridad que no puedan ser modificados, retirados o eludidos sin autorización por los miembros del personal o los proveedores terceros de servicios de TIC,

   iii) el requisito de utilizar dispositivos de almacenamiento de datos extraíbles únicamente cuando el riesgo residual relacionado con las TIC permanezca dentro del nivel de tolerancia al riesgo de la entidad financiera a que se refiere el artículo 3, apartado 1, letra a);

g) el proceso para la supresión segura de los datos que se encuentren en los locales de la entidad financiera o estén almacenados externamente y que la entidad financiera ya no necesite recopilar o almacenar;

h) el proceso para desechar o desactivar de forma segura los dispositivos de almacenamiento de datos que se encuentren en los locales de la entidad financiera o estén almacenados externamente y que contengan información confidencial;

i) la determinación y aplicación de medidas de seguridad para prevenir la pérdida y fuga de datos en relación con los sistemas y dispositivos de nodo final;

j) la aplicación de medidas de seguridad para garantizar que el teletrabajo y el uso de dispositivos de nodo final privados no incidan negativamente en la seguridad de las TIC de la entidad financiera;

k) en el caso de los activos o servicios de TIC explotados por un proveedor tercero de servicios de TIC, la determinación y aplicación de requisitos para mantener la resiliencia operativa digital, de conformidad con los resultados de la clasificación de datos y la evaluación del riesgo relacionado con las TIC.

A efectos de la letra b), la configuración segura de referencia contemplada en dicha letra tendrá en cuenta las prácticas punteras y las técnicas adecuadas establecidas en las normas que se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012.

A efectos de la letra k), las entidades financieras tendrán en cuenta lo siguiente:

a) la aplicación de los parámetros recomendados por los proveedores en los elementos explotados por la entidad financiera;

b) una distribución clara de funciones y responsabilidades en materia de seguridad de la información entre la entidad financiera y el proveedor tercero de servicios de TIC, de conformidad con el principio de plena responsabilidad de la entidad financiera respecto de su proveedor tercero de servicios de TIC a que se refiere el artículo 28, apartado 1, letra a), del Reglamento (UE) 2022/2554, y, en el caso de las entidades financieras a que se refiere el artículo 28, apartado 2, del mismo Reglamento, de conformidad con la política de la entidad financiera sobre el uso de servicios de TIC que sustentan funciones esenciales o importantes;

c) la necesidad de garantizar y mantener las competencias adecuadas dentro de la entidad financiera en lo referente a la gestión y seguridad del servicio utilizado;

d) medidas técnicas y organizativas destinadas a minimizar los riesgos relacionados con la infraestructura utilizada por el proveedor tercero para prestar sus servicios de TIC, teniendo en cuenta las prácticas punteras y las normas definidas en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012.

Artículo 12

Registros

1. Dentro de las salvaguardias contra las intrusiones y el uso indebido de los datos, las entidades financieras elaborarán, documentarán y aplicarán procedimientos, protocolos y herramientas de registro.

2. Los procedimientos, protocolos y herramientas de registro a que se refiere el apartado 1 contendrán todos los aspectos siguientes:

a) la determinación de los hechos que deben registrarse, el período de conservación de los registros y las medidas para proteger y gestionar los datos de los registros, teniendo en cuenta la finalidad para la que se crean tales registros;

b) la correspondencia entre el nivel de detalle de los registros y su finalidad y uso, a fin de permitir la detección eficaz de las actividades anómalas a que se refiere el artículo 24;

c) el requisito de registrar los hechos relacionados con todos los aspectos siguientes:

   i) el control del acceso lógico y físico a que se refiere el artículo 21 y la gestión de la identidad,

   ii) la gestión de la capacidad,

   iii) la gestión de cambios,

   iv) las operaciones de TIC, incluidas las actividades de los sistemas de TIC,

   v) las actividades de tráfico de red, incluido el rendimiento de las redes de TIC;

d) medidas para proteger los sistemas de registro y la información de los registros contra la manipulación, la supresión y el acceso no autorizado en reposo, en tránsito y, en su caso, en uso;

e) medidas para detectar fallos en los sistemas de registro;

f) sin perjuicio de los requisitos normativos aplicables en virtud del Derecho de la Unión o nacional, la sincronización de los relojes de cada uno de los sistemas de TIC de la entidad financiera con una fuente de tiempo de referencia fiable y documentada.

A efectos de la letra a), las entidades financieras establecerán el período de conservación teniendo en cuenta los objetivos empresariales y de seguridad de la información, el motivo por el que se registra el correspondiente hecho y los resultados de la evaluación del riesgo relacionado con las TIC.

Sección 6

Seguridad de las redes

Artículo 13

Gestión de la seguridad de las redes

Dentro de las salvaguardias que garanticen la seguridad de las redes contra las intrusiones y el uso indebido de los datos, las entidades financieras elaborarán, documentarán y aplicarán políticas, procedimientos, protocolos y herramientas en materia de gestión de la seguridad de las redes que incluirán todos los aspectos siguientes:

a) la separación y segmentación de los sistemas y redes de TIC teniendo en cuenta:

   i) el carácter esencial o la importancia de la función sustentada por dichos sistemas y redes de TIC,

   ii) la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554,

   iii) el perfil de riesgo general de los activos de TIC que utilicen dichos sistemas y redes de TIC;

b) la documentación de todas las conexiones de red y flujos de datos de la entidad financiera;

c) el uso de una red separada y específica para la administración de los activos de TIC;

d) la determinación y aplicación de controles de acceso a las redes para prevenir y detectar las conexiones a la red de la entidad financiera mediante cualquier dispositivo o sistema no autorizado o cualquier nodo final que no cumpla los requisitos de seguridad de la entidad financiera;

e) el cifrado de las conexiones de red que pasen por redes corporativas, redes públicas, redes domésticas, redes de terceros y redes inalámbricas, en lo referente a los protocolos de comunicación utilizados, teniendo en cuenta los resultados de la clasificación de datos aprobada, los resultados de la evaluación del riesgo relacionado con las TIC y el cifrado de las conexiones de red a que se refiere el artículo 6, apartado 2;

f) el diseño de las redes en consonancia con los requisitos de seguridad de las TIC establecidos por la entidad financiera, teniendo en cuenta las prácticas punteras para garantizar la confidencialidad, integridad y disponibilidad de las redes;

g) la protección del tráfico de red entre las redes internas e internet y otras conexiones externas;

h) la determinación de las funciones y responsabilidades y de las etapas para la especificación, aplicación, aprobación, modificación y revisión de las reglas cortafuegos y los filtros de conexión;

i) la revisión de la arquitectura de las redes y del diseño de la seguridad de las redes una vez al año, y periódicamente en el caso de las microempresas, con el fin de detectar posibles vulnerabilidades;

j) las medidas para aislar temporalmente, en caso necesario, las subredes y los componentes y dispositivos de red;

k) la aplicación de una configuración segura de referencia de todos los componentes de las redes y el endurecimiento de las redes y de los dispositivos de red en consonancia con las instrucciones de los proveedores, las normas definidas en el artículo 2, punto 1, del Reglamento (UE) n.º 1025/2012, en su caso, y las prácticas punteras;

l) los procedimientos para limitar, bloquear y cerrar las sesiones de sistema y a distancia tras un período de inactividad especificado;

m) respecto de los acuerdos de servicios de red:

   i) la determinación y especificación de las medidas de seguridad de las TIC y de la información, los niveles de servicio y los requisitos de gestión de todos los servicios de red,

   ii) la especificación de si dichos servicios son prestados por un proveedor intragrupo o por proveedores terceros de servicios de TIC.

A efectos de la letra h), las entidades financieras revisarán periódicamente las reglas cortafuegos y los filtros de conexión teniendo en cuenta la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554 y el perfil de riesgo general de los sistemas de TIC que intervengan. En el caso de los sistemas de TIC que sustenten funciones esenciales o importantes, las entidades financieras verificarán la adecuación de las reglas cortafuegos y los filtros de conexión vigentes al menos cada seis meses.

Artículo 14

Protección de la información en tránsito

1. Dentro de las salvaguardias para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, las entidades financieras elaborarán, documentarán y aplicarán políticas, procedimientos, protocolos y herramientas para proteger la información en tránsito. Las entidades financieras garantizarán, en particular, lo siguiente:

a) la disponibilidad, autenticidad, integridad y confidencialidad de los datos durante las transmisiones en red y el establecimiento de procedimientos para evaluar el cumplimiento de tales requisitos;

b) la prevención y detección de fugas de datos y la transferencia segura de información entre la entidad financiera y las partes externas;

c) la aplicación de requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la entidad financiera en materia de protección de la información, en relación con el personal tanto de la entidad financiera como de terceros, y la documentación y revisión periódica de dichos requisitos o acuerdos.

2. Las entidades financieras diseñarán las políticas, procedimientos, protocolos y herramientas para la protección de la información en tránsito a que se refiere el apartado 1 basándose en los resultados de la clasificación de datos aprobada y de la evaluación del riesgo relacionado con las TIC.

Sección 7

Gestión de proyectos de TIC y de cambios en las TIC

Artículo 15

Gestión de proyectos de TIC

1. Dentro de las salvaguardias para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, las entidades financieras elaborarán, documentarán y aplicarán una política de gestión de proyectos de TIC.

2. La política de gestión de proyectos de TIC a que se refiere el apartado 1 especificará los elementos que garanticen la gestión eficaz de los proyectos de TIC relacionados con la adquisición, el mantenimiento y, en su caso, el desarrollo de los sistemas de TIC de la entidad financiera.

3. La política de gestión de proyectos de TIC a que se refiere el apartado 1 contendrá todos los aspectos siguientes:

a) objetivos de los proyectos de TIC;

b) gobernanza de los proyectos de TIC, en particular las funciones y responsabilidades;

c) planificación, calendario y etapas de los proyectos de TIC;

d) evaluación de los riesgos de los proyectos de TIC;

e) hitos pertinentes;

f) requisitos en materia de gestión de los cambios;

g) sometimiento a prueba de todos los requisitos, entre ellos los requisitos de seguridad, y proceso correspondiente de aprobación para la implementación de un sistema de TIC en el entorno de producción.

4. La política de gestión de proyectos de TIC a que se refiere el apartado 1 garantizará la ejecución segura de los proyectos de TIC mediante la facilitación, por el sector o las funciones empresariales a los que afecte el proyecto de TIC, de la información y los conocimientos especializados necesarios.

5. De conformidad con la evaluación de los riesgos de los proyectos de TIC contemplada en el apartado 3, letra d), la política de gestión de proyectos de TIC a que se refiere el apartado 1 dispondrá la obligación de informar al órgano de dirección, tal como se indica a continuación, de la puesta en marcha y el avance de los proyectos de TIC que afecten a funciones esenciales o importantes de la entidad financiera, así como de los riesgos asociados a tales proyectos:

a) de forma individual o agregada, dependiendo de la importancia y las dimensiones de los proyectos de TIC;

b) periódicamente y, en caso necesario, en función de hechos específicos.

Artículo 16

Adquisición, desarrollo y mantenimiento de los sistemas de TIC

1. Dentro de las salvaguardias para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, las entidades financieras elaborarán, documentarán y aplicarán una política que regule la adquisición, el desarrollo y el mantenimiento de sistemas de TIC. Dicha política:

a) determinará las prácticas de seguridad y las metodologías relacionadas con la adquisición, el desarrollo y el mantenimiento de sistemas de TIC;

b) exigirá la determinación de:

   i) especificaciones técnicas y especificaciones técnicas de las TIC en el sentido del artículo 2, puntos 4 y 5, del Reglamento (UE) n.º 1025/2012,

   ii) requisitos relativos a la adquisición, desarrollo y mantenimiento de sistemas de TIC, prestando especial atención a los requisitos de seguridad de las TIC y a su aprobación por la función empresarial pertinente y el propietario de los activos de TIC de conformidad con los mecanismos de gobernanza interna de la entidad financiera;

c) especificará medidas para mitigar el riesgo de alteración no intencionada o de manipulación intencionada de los sistemas de TIC durante su desarrollo, mantenimiento e implementación en el entorno de producción.

2. Las entidades financieras elaborarán, documentarán y aplicarán un procedimiento de adquisición, desarrollo y mantenimiento de sistemas de TIC a efectos de la prueba y aprobación de todos los sistemas de TIC antes de su uso y después del mantenimiento, de conformidad con el artículo 8, apartado 2, letra b), incisos v), vi) y vii). El nivel de las pruebas será acorde con el carácter esencial de los procedimientos empresariales y los activos de TIC afectados. Las pruebas estarán diseñadas con el objetivo de verificar la idoneidad de los nuevos sistemas de TIC para funcionar según lo previsto, así como la calidad del *software* desarrollado internamente.

Además de los requisitos establecidos en el párrafo primero, las entidades de contrapartida central asociarán al diseño y la realización de las pruebas a que se refiere dicho párrafo, según proceda, a:

a) los miembros compensadores y clientes;

b) las entidades de contrapartida central interoperables;

c) otras partes interesadas.

Además de los requisitos establecidos en el párrafo primero, los depositarios centrales de valores asociarán al diseño y la realización de las pruebas a que se refiere dicho párrafo, según proceda, a:

a) los usuarios;

b) los prestadores de servicios esenciales;

c) otros depositarios centrales de valores;

d) otras infraestructuras del mercado;

e) otras entidades con respecto a las cuales hayan determinado la existencia de interdependencias en el marco de su política de continuidad de la actividad.

3. El procedimiento a que se refiere el apartado 2 incluirá la realización de revisiones de códigos fuente que abarquen pruebas tanto estáticas como dinámicas. Dichas pruebas incluirán pruebas de seguridad de los sistemas y aplicaciones expuestos a internet de conformidad con el artículo 8, apartado 2, letra b), incisos v), vi) y vii). Las entidades financieras deberán:

a) identificar y analizar las vulnerabilidades y anomalías en el código fuente;

b) adoptar un plan de acción para hacer frente a esas vulnerabilidades y anomalías;

c) hacer un seguimiento de la aplicación de dicho plan de acción.

4. El procedimiento a que se refiere el apartado 2 incluirá pruebas de seguridad de los paquetes de *software* a más tardar en la fase de integración, de conformidad con el artículo 8, apartado 2, letra b), incisos v), vi) y vii).

5. El procedimiento a que se refiere el apartado 2 dispondrá que:

a) los entornos distintos del de producción únicamente almacenarán datos de producción anonimizados, seudonimizados o aleatorizados;

b) las entidades financieras deberán proteger la integridad y la confidencialidad de los datos en los entornos distintos del de producción.

6. No obstante lo dispuesto en el apartado 5, el procedimiento a que se refiere el apartado 2 podrá disponer que los datos de producción se almacenen únicamente para la realización de pruebas específicas, durante un tiempo limitado y previa aprobación de la función pertinente, y que dichas pruebas se notifiquen a la función de gestión del riesgo relacionado con las TIC.

7. El procedimiento a que se refiere el apartado 2 incluirá la aplicación de controles para proteger la integridad del código fuente de los sistemas de TIC desarrollados internamente o desarrollados y entregados a la entidad financiera por un proveedor tercero de servicios de TIC.

8. El procedimiento a que se refiere el apartado 2 dispondrá que el *software* propietario y, cuando sea factible, el código fuente proporcionado por proveedores terceros de servicios de TIC o procedente de proyectos de código abierto se analizarán y someterán a prueba de conformidad con el apartado 3 antes de su implementación en el entorno de producción.

9. Los apartados 1 a 8 del presente artículo se aplicarán también a los sistemas de TIC desarrollados o gestionados por usuarios ajenos a la función de TIC, utilizando un enfoque basado en el riesgo.

Artículo 17

Gestión de cambios en las TIC

1. Como parte de las salvaguardias para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, las entidades financieras incluirán en los procedimientos de gestión de cambios en las TIC a que se refiere el artículo 9, apartado 4, letra e), del Reglamento (UE) 2022/2554, en relación con todos los cambios en el *software*, el *hardware*, los componentes de *firmware*, los sistemas o los parámetros de seguridad, todos los elementos siguientes:

a) la verificación del cumplimiento de los requisitos de seguridad de las TIC;

b) mecanismos para garantizar la independencia de las funciones que aprueban los cambios y las funciones responsables de solicitar y aplicar dichos cambios;

c) una descripción clara de las funciones y responsabilidades a fin de garantizar:

   i) la especificación y planificación de los cambios,

   ii) el diseño de una transición adecuada,

   iii) el sometimiento a prueba y la ultimación de los cambios de manera controlada,

   iv) la existencia de un aseguramiento eficaz de la calidad;

d) la documentación y comunicación de los detalles de los cambios, en particular:

   i) el objeto y alcance de los cambios,

   ii) el calendario para la aplicación de los cambios,

   iii) los resultados esperados;

e) la determinación de responsabilidades y procedimientos alternativos, en particular responsabilidades y procedimientos para abortar un cambio o recuperarse de un cambio que no se ha ejecutado correctamente;

f) procedimientos, protocolos y herramientas para gestionar los cambios de emergencia que ofrezcan las salvaguardias adecuadas;

g) procedimientos para documentar, reexaminar, evaluar y aprobar los cambios de emergencia tras su aplicación, incluidas las soluciones alternativas y los parches;

h) la determinación de las posibles repercusiones de un cambio sobre las medidas de seguridad de las TIC vigentes, y la evaluación de si dicho cambio requiere la adopción de medidas de seguridad de las TIC adicionales.

2. Tras la introducción de cambios significativos en sus sistemas de TIC, las entidades de contrapartida central y los depositarios centrales de valores someterán tales sistemas a pruebas estrictas mediante la simulación de condiciones de tensión.

Las entidades de contrapartida central asociarán al diseño y la realización de las pruebas a que se refiere el párrafo primero, según proceda, a:

a) los miembros compensadores y clientes;

b) las entidades de contrapartida central interoperables;

c) otras partes interesadas.

Los depositarios centrales de valores asociarán al diseño y la realización de las pruebas a que se refiere el párrafo primero, según proceda, a:

a) los usuarios;

b) los prestadores de servicios esenciales;

c) otros depositarios centrales de valores;

d) otras infraestructuras del mercado;

e) otras entidades con respecto a las cuales hayan determinado la existencia de interdependencias en el marco de su política de continuidad de la actividad en materia de TIC.

Sección 8

Artículo 18

Seguridad física y del entorno

1. Dentro de las salvaguardias para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, las entidades financieras especificarán, documentarán y aplicarán una política de seguridad física y del entorno. Las entidades financieras diseñarán dicha política a la luz del panorama de las ciberamenazas, teniendo en cuenta la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554, y a la luz del perfil de riesgo general de los activos de TIC y los activos de información accesibles.

2. La política de seguridad física y del entorno a que se refiere el apartado 1 contendrá todos los aspectos siguientes:

a) una referencia a la parte de la política sobre el control de los derechos de gestión de accesos a que se refiere el artículo 21, apartado 1, letra g);

b) medidas para proteger contra ataques, accidentes y amenazas y peligros naturales los locales, los centros de datos de la entidad financiera y las zonas sensibles designadas determinadas por la entidad financiera en las que se encuentren los activos de TIC y los activos de información;

c) medidas para proteger los activos de TIC, tanto dentro como fuera de los locales de la entidad financiera, teniendo en cuenta los resultados de la evaluación del riesgo relacionado con las TIC respecto de los activos de TIC pertinentes;

d) medidas para garantizar la disponibilidad, autenticidad, integridad y confidencialidad de los activos de TIC, los activos de información y los dispositivos de control del acceso físico de la entidad financiera mediante el mantenimiento adecuado;

e) medidas para preservar la disponibilidad, autenticidad, integridad y confidencialidad de los datos, en particular:

   i) una política de mesas limpias para los documentos,

   ii) una política de pantallas limpias para las instalaciones de tratamiento de información.

A efectos de la letra b), las medidas de protección contra las amenazas y peligros medioambientales serán acordes con la importancia de los locales, los centros de datos y las zonas sensibles designadas y con el carácter esencial de las operaciones que se realicen en ellos o los sistemas de TIC que se encuentren en ellos.

A efectos de la letra c), la política de seguridad física y del entorno a que se refiere el apartado 1 incluirá medidas que garanticen una protección adecuada de los activos de TIC no vigilados.

Capítulo II

Política de recursos humanos y control de acceso

Artículo 19

Política de recursos humanos

Las entidades financieras incluirán en su política de recursos humanos u otras políticas pertinentes todos los elementos relacionados con la seguridad de las TIC que se indican a continuación:

a) la determinación y asignación de toda responsabilidad específica en materia de seguridad de las TIC;

b) los requisitos de que el personal de la entidad financiera y de los proveedores terceros de servicios de TIC que utilice activos de TIC de la entidad financiera o acceda a ellos:

i) esté informado de las políticas, procedimientos y protocolos en materia de seguridad de las TIC de la entidad financiera y se adhiera a ellos,

ii) conozca los canales de denuncia establecidos por la entidad financiera para la detección de comportamientos anómalos, incluidos, en su caso, los canales de denuncia establecidos de conformidad con la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo ([11]),

iii) restituya a la entidad financiera, al término de su relación laboral, todos los activos de TIC y los activos de información tangibles que obren en su poder y pertenezcan a la entidad financiera.

Artículo 20

Gestión de la identidad

1. Dentro de su control de los derechos de gestión de accesos, las entidades financieras elaborarán, documentarán y aplicarán políticas y procedimientos de gestión de la identidad que garanticen la identificación y autenticación únicas de las personas físicas y los sistemas que accedan a su información a fin de poder asignar los derechos de acceso de usuario de conformidad con el artículo 21.

2. Las políticas y procedimientos de gestión de la identidad a que se refiere el apartado 1 incluirán todos los aspectos siguientes:

a) sin perjuicio de lo dispuesto en el artículo 21, apartado 1, letra c), se asignará una identidad única correspondiente a una cuenta de usuario única a cada miembro del personal de la entidad financiera o del personal de los proveedores terceros de servicios de TIC que acceda a los activos de información y los activos de TIC de la entidad financiera;

b) un proceso de gestión de identidades y cuentas a lo largo de su ciclo de vida que gestione la creación, modificación, revisión y actualización, la desactivación temporal y la cancelación de todas las cuentas.

A efectos de la letra a), las entidades financieras llevarán un registro de todas las identidades asignadas. Dicho registro se conservará tras una reorganización de la entidad financiera o una vez finalizada la relación contractual, sin perjuicio de los requisitos de conservación establecidos en el Derecho nacional y de la Unión aplicable.

A efectos de la letra b), las entidades financieras implementarán, cuando sea factible y adecuado, soluciones automatizadas para el proceso de gestión de identidades a lo largo de su ciclo de vida.

Artículo 21

Control de acceso

Dentro de su control de los derechos de gestión de accesos, las entidades financieras elaborarán, documentarán y aplicarán una política que incluya todos los aspectos siguientes:

a) la asignación de derechos de acceso a los activos de TIC sobre la base de los principios de «necesidad de conocer», «necesidad de uso» y «mínimo privilegio», también para el acceso a distancia y de emergencia;

b) la separación de funciones con el fin de impedir el acceso injustificado a datos esenciales o la asignación de combinaciones de derechos de acceso que puedan utilizarse para eludir los controles;

c) una disposición sobre responsabilidad de los usuarios que limite en la medida de lo posible el uso de cuentas de usuario genéricas y compartidas y garantice que, en todo momento, los usuarios sean identificables cuando realicen acciones en los sistemas de TIC;

([11]) Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (DO L 305 de 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) una disposición sobre las restricciones de acceso a los activos de TIC que establezca controles y herramientas para impedir el acceso no autorizado;

e) procedimientos de gestión de cuentas para la concesión, modificación o revocación de derechos de acceso en relación con las cuentas de usuario y las cuentas genéricas, incluidas las cuentas de administrador genéricas, que incluyan disposiciones sobre todos los aspectos siguientes:

   i) asignación de funciones y responsabilidades para la concesión, revisión y revocación de los derechos de acceso,

   ii) asignación de acceso privilegiado, de emergencia y de administrador sobre la base del principio de «necesidad de uso» o con carácter *ad hoc* para todos los sistemas de TIC,

   iii) retirada de los derechos de acceso sin demora indebida al término de la relación laboral o cuando el acceso ya no sea necesario,

   iv) actualización de los derechos de acceso cuando se requiera introducir cambios y al menos una vez al año para todos los sistemas de TIC que no sustenten funciones esenciales o importantes y al menos cada seis meses para los sistemas de TIC que sustenten funciones esenciales o importantes;

f) métodos de autenticación, incluidos todos los aspectos siguientes:

   i) el uso de métodos de autenticación que sean acordes con la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554 y con el perfil de riesgo general de los activos de TIC, y que tengan en cuenta las prácticas punteras,

   ii) el uso de métodos de autenticación sólidos de conformidad con las prácticas y técnicas punteras para el acceso a distancia a la red de la entidad financiera, el acceso privilegiado y el acceso a los activos de TIC que sustenten funciones esenciales o importantes o a los activos de TIC que sean de acceso público;

g) medidas de control del acceso físico que incluyan lo siguiente:

   i) la identificación y el registro de las personas físicas autorizadas a acceder a los locales, los centros de datos y las zonas sensibles designadas determinadas por la entidad financiera en los que se encuentren los activos de TIC y de información,

   ii) la concesión de derechos de acceso físico a los activos de TIC esenciales únicamente a las personas autorizadas, de conformidad con los principios de «necesidad de conocer» y «mínimo privilegio» y con carácter *ad hoc*,

   iii) el seguimiento del acceso físico a los locales, los centros de datos y las zonas sensibles designadas determinadas por la entidad financiera en los que se encuentren los activos de TIC, los activos de información o ambos,

   iv) la revisión de los derechos de acceso físico para garantizar la rápida revocación de los derechos que no sean necesarios.

A efectos de la letra e), inciso i), las entidades financieras establecerán el período de conservación teniendo en cuenta los objetivos empresariales y de seguridad de la información, los motivos por los que se consigna el hecho de que se trate en los registros y los resultados de la evaluación del riesgo relacionado con las TIC.

A efectos de la letra e), inciso ii), las entidades financieras utilizarán, en la medida de lo posible, cuentas específicas para la realización de tareas administrativas en los sistemas de TIC. Cuando sea factible y adecuado, las entidades financieras implementarán soluciones automatizadas para la gestión del acceso privilegiado.

A efectos de la letra g), inciso i), la identificación y el registro serán acordes con la importancia de los locales, los centros de datos y las zonas sensibles designadas y con el carácter esencial de las operaciones que se realicen en ellos o los sistemas de TIC que se encuentren en ellos.

A efectos de la letra g), inciso iii), el seguimiento será acorde con la clasificación establecida de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2022/2554 y con el carácter esencial de la zona a la que se acceda.

CAPÍTULO III

Detección de incidentes relacionados con las TIC y respuesta a tales incidentes

Artículo 22

Política de gestión de incidentes relacionados con las TIC

Dentro de los mecanismos para la detección de actividades anómalas, incluidos los problemas de rendimiento de las redes de TIC y los incidentes relacionados con las TIC, las entidades financieras elaborarán, documentarán y aplicarán una política de incidentes relacionados con las TIC en virtud de la cual:

a) documentarán el proceso de gestión de incidentes relacionados con las TIC a que se refiere el artículo 17 del Reglamento (UE) 2022/2554;

b) establecerán una lista de los contactos pertinentes con las funciones internas y las partes interesadas externas que participen directamente en la seguridad de las operaciones de TIC, en particular por lo que respecta a:

   i) la detección y el seguimiento de las ciberamenazas,

   ii) la detección de actividades anómalas,

   iii) la gestión de vulnerabilidades;

c) establecerán, implementarán y aplicarán mecanismos técnicos, organizativos y operativos en apoyo del proceso de gestión de incidentes relacionados con las TIC, en particular mecanismos que permitan la rápida detección de actividades y comportamientos anómalos de conformidad con el artículo 23 del presente Reglamento;

d) conservarán todas las pruebas sobre los incidentes relacionados con las TIC por un período no superior al necesario para los fines con los que se hayan recopilado los datos y acorde con el carácter esencial de las funciones empresariales, los procesos de apoyo y los activos de información y de TIC afectados, de conformidad con el [artículo [15] del Reglamento Delegado (UE) 2024/1772 de la Comisión ([12]) y con cualquier requisito de conservación aplicable en virtud del Derecho de la Unión;

e) establecerán y aplicarán mecanismos para analizar los incidentes relacionados con las TIC significativos o recurrentes y los patrones en el número y la frecuencia de los incidentes relacionados con las TIC.

A efectos de la letra d), las entidades financieras conservarán las pruebas a que se refiere dicha letra de manera segura.

Artículo 23

Detección de actividades anómalas y criterios para detectar y responder a incidentes relacionados con las TIC

1. Las entidades financieras establecerán funciones y responsabilidades claras para detectar incidentes relacionados con las TIC y actividades anómalas, así como para responder a tales incidentes y actividades, de manera eficaz.

2. El mecanismo para detectar rápidamente las actividades anómalas, incluidos los problemas de rendimiento de las redes de TIC y los incidentes relacionados con las TIC, a que se refiere el artículo 10, apartado 1, del Reglamento (UE) 2022/2554 permitirá a las entidades financieras:

a) recopilar, analizar y hacer un seguimiento de todos los aspectos siguientes:

   i) factores internos y externos, incluidos, como mínimo, los registros recopilados de conformidad con el artículo 12 del presente Reglamento, la información de las funciones empresariales y de TIC, y los problemas notificados por los usuarios de la entidad financiera,

   ii) posibles ciberamenazas internas y externas, teniendo en cuenta los escenarios utilizados habitualmente por los agentes de riesgo y los escenarios basados en actividades de inteligencia sobre amenazas,

([12]) Reglamento Delegado (UE) 2024/1772 de la Comisión, de 13 de marzo de 2024, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo mediante normas técnicas de regulación que especifican los criterios para la clasificación de los incidentes relacionados con las TIC y las ciberamenazas, establecen umbrales de importancia relativa y especifican la información detallada de las notificaciones de incidentes graves (DO L 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) notificación por un proveedor tercero de servicios de TIC de la entidad financiera de incidentes relacionados con las TIC detectados en las redes y sistemas de TIC del proveedor que puedan afectar a la entidad financiera;

b) detectar actividades y comportamientos anómalos e introducir herramientas que generen alertas sobre dichas actividades y comportamientos, al menos para los activos de TIC y los activos de información que sustenten funciones esenciales o importantes;

c) dar prioridad a las alertas a que se refiere la letra b) para que los incidentes relacionados con las TIC detectados puedan gestionarse dentro del tiempo de resolución previsto, según lo especificado por las entidades financieras, tanto dentro como fuera del horario laboral;

d) registrar, analizar y evaluar, de forma manual o automática, toda información pertinente sobre las actividades y comportamientos anómalos.

A efectos de la letra b), las herramientas a que se refiere dicha letra incluirán herramientas que proporcionen alertas automatizadas sobre la base de reglas predefinidas para detectar las anomalías que afecten a la exhaustividad e integridad de las fuentes de datos o a la recogida de registros.

3. Las entidades financieras protegerán los registros de las actividades anómalas contra la manipulación y el acceso no autorizado en reposo, en tránsito y, en su caso, en uso.

4. Las entidades financieras registrarán, respecto de cada actividad anómala detectada, toda la información pertinente para:

a) determinar la fecha y hora en que se haya producido la actividad anómala;

b) determinar la fecha y hora en que se haya detectado la actividad anómala;

c) determinar el tipo de actividad anómala.

5. Las entidades financieras tendrán en cuenta todos los criterios que se indican a continuación para activar los procesos destinados a detectar y responder a incidentes relacionados con las TIC a que se refiere el artículo 10, apartado 2, del Reglamento (UE) 2022/2554:

a) indicios de que puede haberse llevado a cabo una actividad malintencionada en una red o sistema de TIC, o de que dicha red o sistema de TIC puede haberse visto comprometido;

b) detección de pérdidas de datos en relación con la disponibilidad, autenticidad, integridad y confidencialidad de los datos;

c) detección de efectos adversos en las transacciones y operaciones de la entidad financiera;

d) indisponibilidad de las redes y sistemas de TIC.

6. A efectos del apartado 5, las entidades financieras también tendrán en cuenta el carácter esencial de los servicios afectados.

CAPÍTULO IV

Gestión de la continuidad de la actividad en materia de TIC

Artículo 24

Componentes de la política de continuidad de la actividad en materia de TIC

1. Las entidades financieras incluirán en su política de continuidad de la actividad en materia de TIC a que se refiere el artículo 11, apartado 1, del Reglamento (UE) 2022/2554 todos los elementos siguientes:

a) una descripción de:

i) los objetivos de la política de continuidad de la actividad en materia de TIC, incluida la interrelación entre la continuidad de la actividad en sentido global y la continuidad de la actividad en materia de TIC, y teniendo en cuenta los resultados del análisis de impacto en el negocio a que se refiere el artículo 11, apartado 5, del Reglamento (UE) 2022/2554,

ii) el alcance de las disposiciones, planes, procedimientos y mecanismos para la continuidad de la actividad en materia de TIC, incluidas las limitaciones y exclusiones,

iii) el período que deben cubrir las disposiciones, planes, procedimientos y mecanismos para la continuidad de la actividad en materia de TIC,

iv) los criterios para activar y desactivar los planes de continuidad de la actividad en materia de TIC, los planes de respuesta y recuperación en materia de TIC y los planes de comunicación de crisis;

b) disposiciones sobre:

i) la gobernanza y organización para aplicar la política de continuidad de la actividad en materia de TIC, en particular las funciones y responsabilidades y los procedimientos de traslado a la instancia jerárquica superior que garanticen la disponibilidad de recursos suficientes,

ii) la armonización entre los planes de continuidad de la actividad en materia de TIC y los planes globales de continuidad de la actividad, en relación, como mínimo, con todos los aspectos siguientes:

1) posibles escenarios de fallo, en particular los escenarios a que se refiere el artículo 26, apartado 2, del presente Reglamento;

2) objetivos de recuperación, con la especificación de que, tras sufrir perturbaciones, la entidad financiera debe ser capaz de recuperar las operaciones de sus funciones esenciales o importantes dentro de un objetivo de tiempo de recuperación y un objetivo de punto de recuperación,

iii) la elaboración, dentro de dichos planes, de planes de continuidad de la actividad en materia de TIC para el caso de perturbaciones graves de la actividad, y la priorización de las acciones de continuidad de la actividad en materia de TIC utilizando un enfoque basado en el riesgo,

iv) la elaboración, sometimiento a prueba y revisión de planes de respuesta y recuperación en materia de TIC, de conformidad con los artículos 25 y 26 del presente Reglamento,

v) la revisión de la eficacia de las disposiciones, planes, procedimientos y mecanismos para la continuidad de la actividad en materia de TIC aplicados, de conformidad con el artículo 26 del presente Reglamento,

vi) la armonización de la política de continuidad de la actividad en materia de TIC con:

1) la política de comunicación a que se refiere el artículo 14, apartado 2, del Reglamento (UE) 2022/2554;

2) las acciones de comunicación y comunicación de crisis a que se refiere el artículo 11, apartado 2, letra e), del Reglamento (UE) 2022/2554.

2. Además de los requisitos a que se refiere el apartado 1, las entidades de contrapartida central velarán por que su política de continuidad de la actividad en materia de TIC:

a) establezca un tiempo máximo de recuperación de sus funciones esenciales no superior a dos horas;

b) tenga en cuenta los vínculos externos y las interdependencias existentes dentro de la infraestructura financiera, incluidos los centros de negociación de cuya compensación se encargue la entidad de contrapartida central, los sistemas de pago y de liquidación de valores y las entidades de crédito utilizadas por la entidad de contrapartida central o una entidad de contrapartida central vinculada;

c) exija que se establezcan mecanismos para:

i) garantizar la continuidad de las funciones esenciales o importantes de la entidad de contrapartida central sobre la base de escenarios de catástrofe,

ii) mantener un centro de tratamiento secundario capaz de garantizar la continuidad de las funciones esenciales o importantes de la entidad de contrapartida central del mismo modo que el centro principal,

iii) mantener un centro secundario de actividad, o tener acceso inmediato a él, para permitir al personal garantizar la continuidad del servicio en caso de que no pueda disponerse del emplazamiento principal de la actividad,

iv) estudiar la necesidad de contar con centros de tratamiento adicionales, en particular si la diversidad de los perfiles de riesgo de los centros principal y secundario no ofrece suficiente seguridad en cuanto al cumplimiento de los objetivos de continuidad de la actividad de la entidad de contrapartida central en todos los escenarios.

A efectos de la letra a), las entidades de contrapartida central realizarán los pagos y procedimientos de cierre de jornada en cualquier circunstancia en el día y la hora previstos.

A efectos de la letra c), inciso i), los mecanismos a que se refiere dicho inciso contemplarán la disponibilidad de recursos humanos adecuados, el tiempo máximo de paralización de las funciones esenciales y el traspaso para recuperación a un centro secundario.

A efectos de la letra c), inciso ii), el centro de tratamiento secundario a que se refiere dicha letra tendrá un perfil de riesgo geográfico distinto al del centro principal.

3. Además de los requisitos a que se refiere el apartado 1, los depositarios centrales de valores velarán por que su política de continuidad de la actividad en materia de TIC:

a) tenga en cuenta los vínculos e interdependencias con los usuarios, los prestadores de servicios esenciales, otros depositarios centrales de valores y otras infraestructuras del mercado;

b) exija que sus mecanismos de continuidad de la actividad en materia de TIC garanticen que el objetivo de tiempo de recuperación de sus funciones esenciales o importantes no sea superior a dos horas.

4. Además de los requisitos a que se refiere el apartado 1, los centros de negociación velarán por que su política de continuidad de la actividad en materia de TIC garantice:

a) que la negociación puede reanudarse antes de que transcurran dos horas desde que se produzca un incidente perturbador, o en un plazo cercano;

b) que la cantidad máxima de datos que puedan perderse en cualquier servicio informático del centro de negociación después de un incidente perturbador sea próxima a cero.

Artículo 25

Pruebas de los planes de continuidad de la actividad en materia de TIC

1. Al someter a prueba los planes de continuidad de la actividad en materia de TIC de conformidad con el artículo 11, apartado 6, del Reglamento (UE) 2022/2554, las entidades financieras tendrán en cuenta su análisis de impacto en el negocio y la evaluación del riesgo relacionado con las TIC a que se refiere el artículo 3, apartado 1, letra b), del presente Reglamento.

2. Las entidades financieras, mediante las pruebas de los planes de continuidad de la actividad en materia de TIC a que se refiere el apartado 1, evaluarán si dichos planes son capaces de garantizar la continuidad de sus funciones esenciales o importantes. Dichas pruebas:

a) se llevarán a cabo sobre la base de escenarios de prueba que simulen posibles perturbaciones, incluido un conjunto adecuado de escenarios graves pero verosímiles;

b) comprenderán, en su caso, el sometimiento a prueba de los servicios de TIC prestados por proveedores terceros de servicios de TIC;

c) en el caso de las entidades financieras que no sean microempresas, tal como se contempla en el artículo 11, apartado 6, párrafo segundo, del Reglamento (UE) 2022/2554, comprenderán escenarios de conmutación entre la infraestructura primaria de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes;

d) estarán diseñadas para poner en cuestión las hipótesis en las que se basen los planes de continuidad de la actividad, incluidos los mecanismos de gobernanza y los planes de comunicación de crisis;

e) incluirán procedimientos para verificar la capacidad del personal de las entidades financieras, los proveedores terceros de servicios de TIC, los sistemas de TIC y los servicios de TIC para responder de forma adecuada ante los escenarios que han de tenerse debidamente en cuenta de conformidad con el artículo 26, apartado 2.

A efectos de la letra a), las entidades financieras incluirán siempre en las pruebas los escenarios que se hayan tomado en consideración a la hora de elaborar los planes de continuidad de la actividad.

A efectos de la letra b), las entidades financieras tomarán debidamente en consideración los escenarios vinculados a la insolvencia u otros fallos de los proveedores terceros de servicios de TIC o vinculados a riesgos políticos en los países o territorios de tales proveedores, en su caso.

A efectos de la letra c), las pruebas verificarán si al menos las funciones esenciales o importantes pueden desempeñarse adecuadamente durante un período de tiempo suficiente y si es posible restablecer el funcionamiento normal.

3. Además de los requisitos a que se refiere el apartado 2, las entidades de contrapartida central asociarán a las pruebas de los planes de continuidad de la actividad en materia de TIC a que se refiere el apartado 1 a:

a) los miembros compensadores;

b) los proveedores externos;

c) las entidades pertinentes de la infraestructura financiera con respecto a las cuales hayan determinado la existencia de interdependencias en el marco de su política de continuidad de la actividad.

4. Además de los requisitos a que se refiere el apartado 2, los depositarios centrales de valores asociarán a las pruebas de los planes de continuidad de la actividad en materia de TIC a que se refiere el apartado 1, según proceda, a:

a) sus usuarios;

b) los prestadores de servicios esenciales;

c) otros depositarios centrales de valores;

d) otras infraestructuras del mercado;

e) otras entidades con respecto a las cuales hayan determinado la existencia de interdependencias en el marco de su política de continuidad de la actividad.

5. Las entidades financieras documentarán los resultados de las pruebas a que se refiere el apartado 1. Toda deficiencia detectada en las pruebas será objeto de análisis, tratamiento y comunicación al órgano de dirección.

Artículo 26

Planes de respuesta y recuperación en materia de TIC

1. Al elaborar los planes de respuesta y recuperación en materia de TIC a que se refiere el artículo 11, apartado 3, del Reglamento (UE) 2022/2554, las entidades financieras tendrán en cuenta los resultados de su análisis de impacto en el negocio. Dichos planes de respuesta y recuperación en materia de TIC:

a) especificarán las condiciones que motivarán su activación o desactivación, así como toda excepción a dicha activación o desactivación;

b) describirán las medidas que deben adoptarse para garantizar la disponibilidad, integridad, continuidad y recuperación de, al menos, los sistemas y servicios de TIC que sustenten funciones esenciales o importantes de la entidad financiera;

c) estarán concebidos para cumplir los objetivos de recuperación de las operaciones de las entidades financieras;

d) se documentarán y pondrán a disposición del personal que participe en su ejecución y serán fácilmente accesibles en caso de emergencia;

e) contemplarán opciones de recuperación tanto a corto como a largo plazo, incluida la recuperación parcial de los sistemas;

f) establecerán los objetivos que persiguen y las condiciones para considerar que se han ejecutado correctamente.

A efectos de la letra d), las entidades financieras especificarán claramente las funciones y responsabilidades.

2. Los planes de respuesta y recuperación en materia de TIC a que se refiere el apartado 1 determinarán los escenarios pertinentes, entre ellos escenarios de perturbaciones graves en la actividad y de incremento de la probabilidad de que se produzcan perturbaciones. Los escenarios de los planes se elaborarán sobre la base de la información actual en materia de amenazas y las conclusiones extraídas de anteriores perturbaciones de la actividad. Las entidades financieras tendrán debidamente en cuenta todos los escenarios siguientes:

a) ciberataques y conmutaciones entre la infraestructura primaria de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes;

b) 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 escenarios en los que se contemplen debidamente las posibles repercusiones de la insolvencia u otros fallos de cualquier proveedor tercero de servicios de TIC pertinente;

c) fallo parcial o total de los locales, incluidas las oficinas y los locales de uso profesional, y de los centros de datos;

d) fallo importante de los activos de TIC o de la infraestructura de comunicación;

e) indisponibilidad de un número crucial de miembros del personal o de los miembros del personal a cargo de garantizar la continuidad de las operaciones;

f) repercusiones de sucesos relacionados con el cambio climático y la degradación del medio ambiente, catástrofes naturales, pandemias y ataques físicos, como intrusiones y atentados terroristas;

g) ataques internos;

h) inestabilidad política y social, en particular, cuando proceda, en el territorio o país del proveedor tercero de servicios de TIC y en la ubicación en la que se almacenen y traten los datos;

i) cortes de energía generalizados.

3. Los planes de respuesta y recuperación en materia de TIC a que se refiere el apartado 1 contemplarán opciones alternativas ante la eventualidad de que las medidas primarias de recuperación no sean viables a corto plazo debido a los costes, los riesgos, la logística o circunstancias imprevistas.

4. Dentro de los planes de respuesta y recuperación en materia de TIC a que se refiere el apartado 1, las entidades financieras contemplarán y aplicarán medidas de continuidad para mitigar los fallos de los proveedores terceros de servicios de TIC que sustenten funciones esenciales o importantes de dichas entidades.

CAPÍTULO V

Informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC

Artículo 27

Formato y contenido del informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC

1. Las entidades financieras presentarán el informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6, apartado 5, del Reglamento (UE) 2022/2554 en un formato electrónico que permita realizar búsquedas.

2. Las entidades financieras incluirán en el informe a que se refiere el apartado 1 toda la información siguiente:

a) una parte introductoria en la que:

   i) se identificará claramente la entidad financiera objeto del informe y, en su caso, se describirá su estructura de grupo,

   ii) se describirá el contexto del informe atendiendo a la naturaleza, escala y complejidad de los servicios, actividades y operaciones de la entidad financiera, su organización, sus funciones esenciales identificadas, su estrategia, sus principales proyectos o actividades en curso, sus relaciones y su dependencia de servicios y sistemas de TIC internos y contratados, o las implicaciones que tendría una pérdida total o una degradación grave de dichos sistemas para las funciones esenciales o importantes y la eficiencia del mercado,

   iii) se resumirán los principales cambios en el marco de gestión del riesgo relacionado con las TIC desde el anterior informe presentado,

   iv) se ofrecerá un resumen del perfil de riesgo de TIC actual y a corto plazo, el panorama de amenazas, la evaluación de la eficacia de los controles y la postura de ciberseguridad de la entidad financiera,

b) la fecha de aprobación del informe por parte del órgano de dirección de la entidad financiera;

c) una descripción de los motivos para revisar el marco de gestión del riesgo relacionado con las TIC de conformidad con el artículo 6, apartado 5, del Reglamento (UE) 2022/2554;

d) las fechas de inicio y finalización del período de revisión;

e) la indicación de la función responsable de la revisión;

f) una descripción de los principales cambios y mejoras en el marco de gestión del riesgo relacionado con las TIC desde el informe anterior;

g) un resumen de las constataciones de la revisión y un análisis y evaluación detallados de la gravedad de las debilidades, deficiencias y carencias en el marco de gestión del riesgo relacionado con las TIC durante el período de revisión;

h) una descripción de las medidas para tratar las debilidades, deficiencias y carencias detectadas, incluidos todos los aspectos siguientes:

   i) un resumen de las medidas adoptadas para subsanar las debilidades, deficiencias y carencias detectadas,

   ii) la fecha prevista para la aplicación de las medidas y las fechas relativas al control interno de la aplicación, junto con información sobre el estado de la aplicación en la fecha de elaboración del informe, que explique, en su caso, si existe el riesgo de que no se respeten los plazos,

   iii) las herramientas que se vayan a utilizar y la determinación de la función responsable de llevar a cabo las medidas, con indicación de si las herramientas y funciones son internas o externas,

   iv) una descripción de las repercusiones de los cambios previstos en las medidas sobre los recursos presupuestarios, humanos y materiales de la entidad financiera, incluidos los recursos dedicados a la aplicación de cualquier medida correctora,

   v) información sobre el proceso de información a la autoridad competente, en su caso,

   vi) cuando las debilidades, deficiencias o carencias detectadas no sean objeto de medidas correctoras, una explicación detallada de los criterios utilizados para analizar las repercusiones de dichas debilidades, deficiencias o carencias, para evaluar el correspondiente riesgo residual relacionado con las TIC y para aceptar ese riesgo;

i) información sobre la evolución prevista del marco de gestión del riesgo relacionado con las TIC;

j) conclusiones extraídas de la revisión del marco de gestión del riesgo relacionado con las TIC;

k) información sobre revisiones anteriores, en particular:

   i) una lista de las revisiones realizadas hasta la fecha presente,

   ii) en su caso, el estado de aplicación de las medidas correctoras señaladas en el último informe,

   iii) cuando las medidas correctoras previstas en revisiones anteriores hayan demostrado ser ineficaces o hayan dado lugar a problemas inesperados, una descripción del modo en que podrían mejorarse esas medidas correctoras o de esos problemas inesperados;

l) fuentes de información empleadas para elaborar el informe, en particular todas las siguientes:

   i) en el caso de las entidades financieras que no sean microempresas a que se refiere el artículo 6, apartado 6, del Reglamento (UE) 2022/2554, los resultados de las auditorías internas,

   ii) los resultados de las evaluaciones de cumplimiento,

   iii) los resultados de las pruebas de resiliencia operativa digital y, en su caso, los resultados de las pruebas avanzadas de las herramientas, los sistemas y los procesos de TIC sustentadas en pruebas de penetración basadas en amenazas,

   iv) las fuentes externas.

A efectos de la letra c), cuando la revisión se haya iniciado siguiendo instrucciones de las autoridades de supervisión o conclusiones derivadas de las pruebas de la resiliencia operativa digital o los procesos de auditoría pertinentes, el informe incluirá referencias explícitas a dichas instrucciones o conclusiones que permitan conocer el motivo para iniciar la revisión. Cuando la revisión se haya iniciado a raíz de incidentes relacionados con las TIC, el informe incluirá la lista de todos los incidentes relacionados con las TIC junto con el análisis de sus causas subyacentes.

A efectos de la letra f), la descripción incluirá un análisis de las repercusiones de los cambios sobre la estrategia de resiliencia operativa digital, el marco de control interno de las TIC y la gobernanza de la gestión del riesgo relacionado con las TIC de la entidad financiera.

TÍTULO III

MARCO SIMPLIFICADO DE GESTIÓN DEL RIESGO RELACIONADO CON LAS TIC A QUE SE REFIERE EL ARTÍCULO 16, APARTADO 1, DEL REGLAMENTO (UE) 2022/2554

CAPÍTULO I

Marco simplificado de gestión del riesgo relacionado con las TIC

Artículo 28

Gobernanza y organización

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 dispondrán de un marco interno de gobernanza y control que garantice una gestión efectiva y prudente del riesgo relacionado con las TIC para lograr un nivel elevado de resiliencia operativa digital.

2. Dentro de su marco simplificado de gestión del riesgo relacionado con las TIC, las entidades financieras a que se refiere el apartado 1 velarán por que su órgano de dirección:

a) asuma la responsabilidad general de garantizar que el marco simplificado de gestión del riesgo relacionado con las TIC permita realizar la estrategia empresarial de la entidad financiera de conformidad con su apetito de riesgo y que, en ese contexto, se tenga en cuenta el riesgo relacionado con las TIC;

b) defina claramente las funciones y responsabilidades para todas las tareas relacionadas con las TIC;

c) defina los objetivos de seguridad de la información y requisitos en materia de TIC;

d) apruebe, supervise y revise periódicamente:

   i) la clasificación de los activos de información de la entidad financiera a que se refiere el artículo 30, apartado 1, del presente Reglamento, la lista de los principales riesgos detectados y el análisis de impacto en el negocio y las políticas conexas,

   ii) los planes de continuidad de la actividad de la entidad financiera y las medidas de respuesta y recuperación a que se refiere el artículo 16, apartado 1, letra f), del Reglamento (UE) 2022/2554;

e) asigne y revise, al menos una vez al año, el presupuesto necesario para satisfacer las necesidades de resiliencia operativa digital de la entidad financiera con respecto a todos los tipos de recursos, incluidos los pertinentes programas de sensibilización en materia de seguridad de las TIC y las pertinentes actividades de formación sobre resiliencia operativa digital y capacidades en materia de TIC para todo el personal;

f) especifique y aplique las políticas y medidas contempladas en los capítulos I, II y III del presente título para determinar, evaluar y gestionar el riesgo relacionado con las TIC al que está expuesta la entidad financiera;

g) determine y aplique los procedimientos, protocolos y herramientas de TIC necesarios para proteger todos los activos de información y activos de TIC;

h) garantice que el personal de la entidad financiera se mantiene al día con conocimientos y capacidades suficientes para comprender y evaluar el riesgo relacionado con las TIC y sus repercusiones en las operaciones de la entidad financiera, de manera acorde con el riesgo relacionado con las TIC que se esté gestionando;

i) establezca disposiciones sobre presentación de información, en particular la frecuencia, forma y contenido de los informes que se le deban presentar sobre la seguridad de la información y la resiliencia operativa digital.

3. Las entidades financieras a que se refiere el apartado 1 podrán externalizar, de conformidad con el Derecho sectorial de la Unión y nacional, a proveedores intragrupo o terceros de servicios de TIC 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, las entidades financieras seguirán siendo plenamente responsables de la verificación del cumplimiento de los requisitos en materia de gestión del riesgo relacionado con las TIC.

4. Las entidades financieras a que se refiere el apartado 1 garantizarán una separación adecuada, así como la independencia, de las funciones de control y las funciones de auditoría interna.

5. Las entidades financieras a que se refiere el apartado 1 garantizarán que su marco simplificado de gestión del riesgo relacionado con las TIC sea objeto de auditoría interna llevada a cabo por auditores, en consonancia con su plan de auditoría. Los auditores poseerán conocimientos, capacidades y pericia suficientes en materia de riesgo relacionado con las TIC y serán independientes. La frecuencia y el enfoque de las auditorías de TIC serán acordes con el riesgo relacionado con las TIC de la entidad financiera.

6. A la luz del resultado de la auditoría contemplada en el apartado 5, las entidades financieras a que se refiere el apartado 1 velarán por la oportuna verificación y corrección de los resultados problemáticos de la auditoría de TIC.

Artículo 29

Política y medidas de seguridad de la información

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 elaborarán, documentarán y aplicarán una política de seguridad de la información en el contexto del marco simplificado de gestión del riesgo relacionado con las TIC. Dicha política de seguridad de la información especificará los principios y normas de alto nivel para proteger la confidencialidad, integridad, disponibilidad y autenticidad de los datos y de los servicios prestados por esas entidades financieras.

2. Sobre la base de la política de seguridad de la información contemplada en el apartado 1, las entidades financieras a que se refiere dicho apartado establecerán y aplicarán medidas de seguridad de las TIC para mitigar su exposición al riesgo relacionado con las TIC, incluidas medidas de mitigación que aplicarán los proveedores terceros de servicios de TIC.

Las medidas de seguridad de las TIC incluirán todas las medidas contempladas en los artículos 30 a 38.

Artículo 30

Clasificación de activos de información y activos de TIC

1. Dentro del marco simplificado de gestión del riesgo relacionado con las TIC contemplado en el artículo 16, apartado 1, letra a), del Reglamento (UE) 2022/2554, las entidades financieras a que se refiere el apartado 1 de dicho artículo identificarán, clasificarán y documentarán todas las funciones esenciales o importantes, los activos de información y los activos de TIC que sustenten dichas funciones, así como sus interdependencias. Las entidades financieras revisarán los elementos identificados y su clasificación cuando sea necesario.

2. Las entidades financieras a que se refiere el apartado 1 identificarán todas las funciones esenciales o importantes sustentadas por proveedores terceros de servicios de TIC.

Artículo 31

Gestión del riesgo relacionado con las TIC

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 incluirán en su marco simplificado de gestión del riesgo relacionado con las TIC todos los aspectos siguientes:

a) la determinación de los niveles de tolerancia al riesgo relacionado con las TIC, de acuerdo con el apetito de riesgo de la entidad financiera;

b) la determinación y evaluación de los riesgos relacionados con las TIC a los que la entidad financiera esté expuesta;

c) la especificación de las estrategias de mitigación al menos para los riesgos relacionados con las TIC que no entren dentro de los niveles de tolerancia al riesgo de la entidad financiera;

d) el seguimiento de la eficacia de las estrategias de mitigación a que se refiere la letra c);

e) la determinación y evaluación de todo riesgo relacionado con las TIC y la seguridad de la información que sea consecuencia de un cambio importante en los sistemas de TIC o los servicios, procesos o procedimientos de TIC, se derive de los resultados de las pruebas de seguridad de las TIC o surja tras un incidente grave relacionado con las TIC.

2. Las entidades financieras a que se refiere el apartado 1 llevarán a cabo y documentarán la evaluación del riesgo relacionado con las TIC con carácter periódico, de manera acorde con su perfil de riesgo relacionado con las TIC.

3. Las entidades financieras a que se refiere el apartado 1 harán un seguimiento continuo de las amenazas y vulnerabilidades que sean pertinentes para sus funciones esenciales o importantes, así como para sus activos de información y activos de TIC, y revisarán periódicamente los escenarios de riesgo que afecten a dichas funciones esenciales o importantes.

4. Las entidades financieras a que se refiere el apartado 1 establecerán umbrales de alerta y criterios para activar e iniciar procesos de respuesta a incidentes relacionados con las TIC.

Artículo 32

Seguridad física y del entorno

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 determinarán y aplicarán medidas de seguridad física concebidas sobre la base del panorama de amenazas y de conformidad con la clasificación contemplada en el artículo 30, apartado 1, del presente Reglamento, el perfil de riesgo general de los activos de TIC y los activos de información accesibles.

2. Las medidas a que se refiere el apartado 1 protegerán los locales y, en su caso, los centros de datos de las entidades financieras en los que se encuentren los activos de TIC y de información contra el acceso no autorizado, los ataques y los accidentes, así como contra las amenazas y peligros medioambientales.

3. La protección contra las amenazas y peligros medioambientales será acorde con la importancia de los locales afectados y, en su caso, de los centros de datos y con el carácter esencial de las operaciones que se realicen en ellos o los sistemas de TIC que se encuentren en ellos.

CAPÍTULO II

Otros elementos de los sistemas, protocolos y herramientas para minimizar las consecuencias del riesgo relacionado con las TIC

Artículo 33

Control de acceso

Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 elaborarán, documentarán y aplicarán procedimientos para controlar el acceso lógico y físico, velarán por su cumplimiento, los someterán a seguimiento y los revisarán periódicamente. Dichos procedimientos incluirán los siguientes elementos de control del acceso lógico y físico:

a) derechos de acceso a los activos de información, los activos de TIC y las funciones que sustentan, así como a los emplazamientos esenciales de actividad de la entidad financiera, gestionados sobre la base de los principios de «necesidad de conocer», «necesidad de uso» y «mínimo privilegio», también para el acceso a distancia y de emergencia;

b) responsabilidad de los usuarios, en virtud de la cual se garantice la identificación de los usuarios en las acciones realizadas en los sistemas de TIC;

c) procedimientos de gestión de cuentas para la concesión, modificación o revocación de derechos de acceso en relación con las cuentas de usuario y cuentas genéricas, incluidas las cuentas de administrador genéricas;

d) métodos de autenticación acordes con la clasificación a que se refiere el artículo 30, apartado 1, y con el perfil de riesgo general de los activos de TIC, y basados en las prácticas punteras;

e) revisión periódica de los derechos de acceso y retirada de esos derechos cuando ya no sean necesarios.

A efectos de la letra c), la entidad financiera asignará, para todos los activos de TIC, acceso privilegiado, de emergencia y de administrador sobre la base del principio de «necesidad de uso» o con carácter *ad hoc*, y lo registrará de conformidad con el artículo 34, apartado 1, letra f).

A efectos de la letra d), las entidades financieras utilizarán métodos de autenticación fuerte basados en las prácticas punteras para el acceso a distancia a sus redes, el acceso privilegiado y el acceso a los activos de TIC que sustenten funciones esenciales o importantes que sean de acceso público.

Artículo 34

Seguridad de las operaciones de TIC

Dentro de sus sistemas, protocolos y herramientas, y con respecto a todos los activos de TIC, las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554:

a) harán un seguimiento del ciclo de vida de todos los activos de TIC y lo gestionarán;

b) harán un seguimiento, en su caso, de si los activos de TIC cuentan con el soporte de proveedores terceros de servicios de TIC;

c) determinarán los requisitos de capacidad de sus activos de TIC y las medidas para mantener y mejorar la disponibilidad y eficiencia de los sistemas de TIC y prevenir la escasez de capacidad de TIC antes de que se materialice;

d) llevarán a cabo exploraciones y evaluaciones automatizadas de vulnerabilidad de los activos de TIC, acordes con la clasificación de tales activos contemplada en el artículo 30, apartado 1, y con el perfil de riesgo general de cada activo de TIC, e implementarán parches para hacer frente a las vulnerabilidades detectadas;

e) gestionarán los riesgos relacionados con los activos de TIC obsoletos, sin soporte o heredados;

f) registrarán los acontecimientos relacionados con el control del acceso lógico y físico, las operaciones de TIC, incluidas las actividades de sistema y de tráfico de red, y la gestión de cambios en las TIC;

g) determinarán y aplicarán medidas para el seguimiento y el análisis de la información sobre actividades y comportamientos anómalos respecto de operaciones de TIC esenciales o importantes;

h) aplicarán medidas para el seguimiento de la información pertinente y actualizada sobre las ciberamenazas;

i) aplicarán medidas para la detección de posibles fugas de información, códigos maliciosos y otras amenazas para la seguridad, así como vulnerabilidades en el *software* y el *hardware* conocidas públicamente, y comprobarán las nuevas actualizaciones de seguridad correspondientes.

A efectos de la letra f), las entidades financieras adaptarán el grado de detalle de los registros a la finalidad y al uso del activo de TIC que los genere.

Artículo 35

Seguridad de los datos, sistemas y redes

Dentro de sus sistemas, protocolos y herramientas, las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 elaborarán y aplicarán salvaguardias que garanticen la seguridad de las redes frente a intrusiones y al uso indebido de los datos y que preserven la disponibilidad, autenticidad, integridad y confidencialidad de los datos. En particular, teniendo en cuenta la clasificación a que se refiere el artículo 30, apartado 1, del presente Reglamento, las entidades financieras establecerán todos los aspectos siguientes:

a) la determinación y aplicación de medidas para proteger los datos en uso, en tránsito y en reposo;

b) la determinación y aplicación de medidas de seguridad relativas al uso del *software*, los soportes de almacenamiento de datos, los sistemas y los dispositivos de nodo final que transfieran y almacenen datos de la entidad financiera;

c) la determinación y aplicación de medidas para prevenir y detectar las conexiones no autorizadas a sus redes, así como para proteger el tráfico de red entre sus redes internas e internet y otras conexiones externas;

d) la determinación y aplicación de medidas que garanticen la disponibilidad, autenticidad, integridad y confidencialidad de los datos durante las transmisiones en redes;

e) un proceso para la supresión segura de los datos que se encuentren en los locales o estén almacenados externamente y que la entidad financiera ya no necesite recopilar o almacenar;

f) un proceso para desechar o desactivar de forma segura los dispositivos de almacenamiento de datos que se encuentren en los locales o estén almacenados externamente y que contengan información confidencial;

g) la determinación y aplicación de medidas de seguridad para garantizar que el teletrabajo y el uso de dispositivos de nodo final privados no afecten negativamente a la capacidad para llevar a cabo sus actividades esenciales de manera adecuada, oportuna y segura.

Artículo 36

Pruebas de seguridad de las TIC

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 establecerán y aplicarán un plan de pruebas de seguridad de las TIC para validar la eficacia de las medidas de seguridad de las TIC que hayan elaborado de conformidad con los artículos 33, 34, 35, 37 y 38 del presente Reglamento. Las entidades financieras velarán por que dicho plan tenga en cuenta las amenazas y vulnerabilidades detectadas dentro del marco simplificado de gestión del riesgo relacionado con las TIC a que se refiere el artículo 31 del presente Reglamento.

2. Las entidades financieras a que se refiere el apartado 1 revisarán, evaluarán y someterán a prueba las medidas de seguridad de las TIC, tomando en consideración el perfil de riesgo general de sus activos de TIC.

3. Las entidades financieras a que se refiere el apartado 1 harán un seguimiento y una evaluación de los resultados de las pruebas de seguridad y actualizarán sus medidas de seguridad en consecuencia y sin demora indebida en el caso de los sistemas de TIC que sustenten funciones esenciales o importantes.

Artículo 37

Adquisición, desarrollo y mantenimiento de los sistemas de TIC

Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 diseñarán y aplicarán, en su caso, un procedimiento para la adquisición, el desarrollo y el mantenimiento de los sistemas de TIC con arreglo a un enfoque basado en el riesgo. Dicho procedimiento:

a) garantizará que, antes de la adquisición o el desarrollo de un sistema de TIC, los requisitos funcionales y no funcionales, incluidos los requisitos de seguridad de la información, hayan sido claramente especificados y aprobados por la función empresarial pertinente;

b) garantizará que los sistemas de TIC se sometan a prueba y sean aprobados antes de su primera utilización y antes de introducir cambios en el entorno de producción;

c) determinará medidas para mitigar el riesgo de alteración no intencionada o de manipulación intencionada de los sistemas de TIC durante el desarrollo y la implementación en el entorno de producción.

Artículo 38

Gestión de proyectos de TIC y de cambios en las TIC

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 elaborarán, documentarán y aplicarán un procedimiento de gestión de proyectos de TIC y especificarán las funciones y responsabilidades en relación con su aplicación. Dicho procedimiento abarcará todas las fases de los proyectos de TIC, desde su inicio hasta su cierre.

2. Las entidades financieras a que se refiere el apartado 1 elaborarán, documentarán y aplicarán un procedimiento de gestión de cambios en las TIC para garantizar que todo cambio en los sistemas de TIC se registre, someta a prueba, evalúe, apruebe, aplique y verifique de manera controlada y con las salvaguardias adecuadas a fin de preservar la resiliencia operativa digital de la entidad financiera.

CAPÍTULO III

Gestión de la continuidad de la actividad en materia de TIC

Artículo 39

Componentes del plan de continuidad de la actividad en materia de TIC

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 elaborarán sus planes de continuidad de la actividad en materia de TIC teniendo en cuenta los resultados del análisis de sus exposiciones a perturbaciones graves de la actividad, así como de las posibles repercusiones de esas perturbaciones, y los escenarios a los que puedan estar expuestos sus activos de TIC que sustenten funciones esenciales o importantes, en particular un escenario de ciberataque.

2. Los planes de continuidad de la actividad en materia de TIC a que se refiere el apartado 1:

a) serán aprobados por el órgano de dirección de la entidad financiera;

b) estarán documentados y serán fácilmente accesibles en caso de emergencia o crisis;

c) asignarán recursos suficientes para su ejecución;

d) establecerán los niveles de recuperación previstos y los plazos para la recuperación y reanudación de las funciones y las dependencias internas y externas clave, en particular con respecto a los proveedores terceros de servicios de TIC;

e) determinarán las condiciones que pueden motivar su activación y las medidas que deben adoptarse para garantizar la disponibilidad, continuidad y recuperación de los activos de TIC de las entidades financieras que sustenten funciones esenciales o importantes;

f) determinarán las medidas de restauración y recuperación en relación con las funciones empresariales esenciales o importantes, los procesos de apoyo y los activos de información, así como sus interdependencias, con el fin de evitar efectos adversos en el funcionamiento de las entidades financieras;

g) determinarán procedimientos y medidas de copia de seguridad que especifiquen el alcance de los datos objeto de dicha copia y la frecuencia mínima de su realización, de acuerdo con el carácter esencial de la función que utilice los datos de que se trate;

h) contemplarán opciones alternativas ante la eventualidad de que la recuperación no sea viable a corto plazo debido a los costes, los riesgos, la logística o circunstancias imprevistas;

i) especificarán los mecanismos de comunicación interna y externa, incluidos los planes para el traslado a la instancia jerárquica superior;

j) se actualizarán en consonancia con las conclusiones extraídas de incidentes, las pruebas, los nuevos riesgos y amenazas detectados, los cambios en los objetivos de recuperación y los cambios importantes en la organización de la entidad financiera y en los activos de TIC que sustenten funciones esenciales o empresariales.

A efectos de la letra f), las medidas a que se refiere dicha letra contemplarán la mitigación de los fallos de los proveedores terceros esenciales.

Artículo 40

Pruebas de los planes de continuidad de la actividad

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 someterán a prueba los planes de continuidad de la actividad a que se refiere el artículo 39 del presente Reglamento, incluidos los escenarios contemplados en dicho artículo, al menos una vez al año en el caso de los procedimientos de copia de seguridad y restauración, o cada vez que se produzca un cambio importante en el plan de continuidad de la actividad.

2. Las pruebas de los planes de continuidad de la actividad a que se refiere el apartado 1 deberán demostrar que las entidades financieras contempladas en dicho apartado son capaces de mantener la viabilidad de sus actividades hasta que se restablezcan las operaciones esenciales y detectar cualquier deficiencia en dichos planes.

3. Las entidades financieras a que se refiere el apartado 1 documentarán los resultados de las pruebas de los planes de continuidad de la actividad, y toda deficiencia detectada a raíz de dichas pruebas será analizada, tratada y comunicada al órgano de dirección.

CAPÍTULO IV

Informe sobre la revisión del marco simplificado de gestión del riesgo relacionado con las TIC

Artículo 41

Formato y contenido del informe sobre la revisión del marco simplificado de gestión del riesgo relacionado con las TIC

1. Las entidades financieras a que se refiere el artículo 16, apartado 1, del Reglamento (UE) 2022/2554 presentarán el informe sobre la revisión del marco de gestión del riesgo relacionado con las TIC a que se refiere el apartado 2 de dicho artículo en un formato electrónico que permita realizar búsquedas.

2. El informe a que se refiere el apartado 1 incluirá toda la información siguiente:

a) una parte introductoria que contenga:

   i) una descripción del contexto del informe atendiendo a la naturaleza, escala y complejidad de los servicios, actividades y operaciones de la entidad financiera, su organización, sus funciones esenciales identificadas, su estrategia, sus principales proyectos o actividades en curso, sus relaciones y su dependencia de servicios y sistemas de TIC internos y externalizados, o las implicaciones que tendría una pérdida total o una degradación grave de dichos sistemas para las funciones esenciales o importantes y la eficiencia del mercado,

   ii) un resumen del riesgo relacionado con las TIC actual y a corto plazo identificado, el panorama de amenazas, la evaluación de la eficacia de los controles y la postura de ciberseguridad de la entidad financiera,

   iii) información sobre el ámbito objeto del informe,

   iv) un resumen de los principales cambios en el marco de gestión del riesgo relacionado con las TIC desde el informe anterior,

   v) un resumen y una descripción de las repercusiones de los principales cambios en el marco simplificado de gestión del riesgo relacionado con las TIC desde el informe anterior;

b) en su caso, la fecha de aprobación del informe por parte del órgano de dirección de la entidad financiera;

c) una descripción de los motivos de la revisión, incluidos los aspectos siguientes:

   i) cuando la revisión se haya iniciado siguiendo instrucciones de las autoridades de supervisión, las pruebas de dichas instrucciones,

   ii) cuando la revisión se haya iniciado a raíz del acontecimiento de incidentes relacionados con las TIC, la lista de todos esos incidentes con el correspondiente análisis de las causas subyacentes;

d) las fechas de inicio y finalización del período de revisión;

e) la persona responsable de la revisión;

f) un resumen de las constataciones y una autoevaluación de la gravedad de las debilidades, deficiencias y carencias detectadas en el marco de gestión del riesgo relacionado con las TIC durante el período de revisión, junto con un análisis detallado de esas debilidades, deficiencias y carencias;

g) medidas correctoras determinadas para hacer frente a las debilidades, deficiencias y carencias en el marco simplificado de gestión del riesgo relacionado con las TIC y fecha prevista para la aplicación de dichas medidas, incluidas las medidas de respuesta a debilidades, deficiencias y carencias señaladas en informes anteriores, cuando aún no se hayan subsanado;

h) conclusiones generales de la revisión del marco simplificado de gestión del riesgo relacionado con las TIC, incluida la posible evolución prevista de dicho marco.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 42

Entrada en vigor

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

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 13 de marzo de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN