BANCO DE ESPAÑA
Eurosistema

Directrices sobre gestión de riesgos de TIC y de seguridad

(EBA/GL/2019/04)

Estas Directrices de la Autoridad Bancaria Europea (EBA por sus siglas en inglés) se dirigen a las entidades financieras, que, a efectos de estas directrices, son 1) los proveedores de servicios de pago (PSP), según se definen en el artículo 4, apartado 11, de la DSP2; y 2) las entidades, por las que se entienden las entidades de crédito y las empresas de servicios de inversión, según se definen en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.° 575/2013. Las directrices también se aplican a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.° 575/2013, incluido el Banco Central Europeo en lo que respecta a los asuntos relacionados con las funciones que le atribuye el Reglamento (UE) n.° 1024/2013, y a las autoridades competentes a efectos de la DSP2, a las que se hace referencia en el artículo 4, apartado 2, letra i), del Reglamento (UE) n.° 1093/2010.

Las directrices especifican las medidas de gestión de riesgos que las entidades (según se definen en el párrafo anterior) deben adoptar de conformidad con el artículo 74 de la DRC para gestionar sus riesgos de TIC y de seguridad de todas las actividades y que los proveedores de servicios de pago (PSP) deben adoptar, de conformidad con el artículo 95, apartado 1, de la DSP2, para gestionar los riesgos operativos y de seguridad (entendidos como «riesgos de TIC y de seguridad») relativos a los servicios de pago que prestan. Las directrices incluyen requisitos referentes a la seguridad de la información, incluida la ciberseguridad, en la medida en que la información se almacena en los sistemas de TIC.

Las Directrices se distribuyen en un total de ocho títulos, relativos a: (i) el principio de proporcionalidad; (ii) la gobernanza y estrategia; (iii) el marco de gestión de riesgos; (iv) la seguridad de la información; (v) la gestión de las operaciones de TIC; (vi) la gestión de proyectos y de cambios; (vii) la continuidad de negocio; (viii) la gestión de la relación con los usuarios de los servicios de pago.

Estas Directrices han sido desarrolladas por la EBA de acuerdo con lo señalado en el artículo 16 del Reglamento (UE) No 1093/2010. La EBA publicó la versión en inglés de mismas el 28 de noviembre de 2019 y la versión en español el 3 de marzo de 2020. Se aplicarán a partir del 30 de junio de 2020, y su entrada en vigor supondrá la derogación de las *Directrices sobre las medidas de seguridad para los riesgos operativos y de seguridad (*EBA/GL/2017/17) emitidas en 2017.

La Comisión Ejecutiva del Banco de España adoptó como propias estas directrices el día 27 de abril de 2020, en calidad de autoridad competente de la supervisión directa de las entidades de crédito menos significativas en todas las actividades de prestación de servicios distintos de los de pagos.

Directrices

ABE/GL/2019/04

28 de noviembre de 2019

Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad

Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes directrices

1. El presente documento contiene directrices emitidas en virtud del artículo 16 del Reglamento (UE) n.º 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

2. En las directrices se expone el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión Europea en un determinado ámbito. Las autoridades competentes según se definen en el artículo 4, apartado 2, del Reglamento (UE) n.º 1093/2010 y a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las directrices vayan dirigidas principalmente a las entidades.

Requisitos de notificación

3. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el ([dd.mm.aaaa]), si cumplen o se proponen cumplir estas Directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en ese plazo, la ABE considerará que las autoridades competentes no las cumplen. Las notificaciones se presentarán remitiendo el modelo que se encuentra disponible en el sitio web de la ABE a compliance@eba.europa.eu, con la referencia «EBA/GL/2019/04». Las notificaciones serán remitidas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las directrices deberá notificarse igualmente a la ABE.

4. Las notificaciones se publicarán en el sitio web de la ABE, tal como contempla el artículo 16, apartado 3.

[1] 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).

Objeto, ámbito de aplicación y definiciones

Objeto

5. Las presentes directrices se basan en las disposiciones del artículo 74 de la Directiva 2013/36/UE (DRC) en lo que respecta al gobierno interno y se derivan del mandato de elaborar directrices del artículo 95, apartado 3, de la Directiva (UE) 2015/2366 (DSP2).

6. Las presentes directrices especifican las medidas de gestión de riesgos que las entidades financieras (según se definen en el párrafo 9) deben adoptar de conformidad con el artículo 74 de la DRC para gestionar sus riesgos de TIC y de seguridad de todas las actividades y que los proveedores de servicios de pago (PSP según se definen en el párrafo 9) deben adoptar, de conformidad con el artículo 95, apartado 1, de la DSP2, para gestionar los riesgos operativos y de seguridad (entendidos como «riesgos de TIC y de seguridad») relativos a los servicios de pago que prestan. Las directrices incluyen requisitos referentes a la seguridad de la información, incluida la ciberseguridad, en la medida en que la información se almacena en los sistemas de TIC.

Ámbito de aplicación

7. Las presentes directrices se aplican en relación con la gestión de los riesgos de TIC y de seguridad en las entidades financieras (según se definen en el párrafo 9). A efectos de las presentes directrices, la expresión riesgos de TIC y de seguridad se refiere a los riesgos operativos y de seguridad del artículo 95 de la DSP2 para la prestación de servicios de pago.

8. En el caso de los PSP (según se definen en el párrafo 9), las presentes directrices se aplican a la prestación de servicios de pago, de conformidad con el ámbito y el mandato del artículo 95 de la DSP2. En cuanto a las entidades (según se definen en el párrafo 9), las presentes directrices se aplican a todas las actividades que prestan.

Destinatarios

9. Las presentes directrices se dirigen a las entidades financieras, que, a efectos de estas directrices, son 1) los PSP, según se definen en el artículo 4, apartado 11, de la DSP2; y 2) las entidades, por las que se entienden las entidades de crédito y las empresas de servicios de inversión, según se definen en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.° 575/2013. Las directrices también se aplican a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.° 575/2013, incluido el Banco Central Europeo en lo que respecta a los asuntos relacionados con las funciones que le atribuye el Reglamento (UE) n.° 1024/2013, y a las autoridades competentes a efectos de la DSP2, a las que se hace referencia en el artículo 4, apartado 2, letra i), del Reglamento (UE) n.° 1093/2010.

Definiciones

10. Salvo que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE (DRC), el Reglamento (UE) n.° 575/2013 (RRC) y la Directiva (UE) 2015/2366 (DSP2) tienen idéntico significado en estas directrices. Adicionalmente, a efectos de estas directrices se aplicarán las definiciones siguientes:

Riesgo de TIC y de seguridad	Riesgo de pérdida debido a la violación de la confidencialidad, al fallo de la integridad de los sistemas y los datos, a la inadecuación o indisponibilidad de los sistemas y los datos o a la imposibilidad de cambiar las tecnologías de la información (TI) en unos plazos y con unos costes razonables cuando cambian las necesidades del entorno o del negocio (es decir, la agilidad)[2]. Este riesgo incluye riesgos de seguridad resultantes de la inadecuación o el fallo de procesos internos o de sucesos externos, incluido el riesgo de ciberataques o el riesgo derivado de una seguridad física inadecuada.
Órgano de dirección	(a) Para las entidades de crédito y las empresas de servicios de inversión, este término tiene el mismo significado que en la definición del artículo 3, apartado 1, punto 7, de la Directiva 2013/36/UE. (b) Para las entidades de pago o las entidades de dinero electrónico, este término significa los administradores o las personas responsables de la gestión de las entidades de pago o las entidades de dinero electrónico y, en su caso, las personas responsables de la gestión de las actividades de servicios de pago de las entidades de pago y entidades de dinero electrónico. (c) Para los PSP mencionados en las letras c), e) y f) del artículo 1, apartado 1, de la Directiva (UE) 2015/2366, este término tiene el significado que le confiere la legislación nacional o la legislación de la Unión Europea aplicable.
Incidente operativo o de seguridad	Evento particular o serie de eventos vinculados no planificados por la entidad financiera que tengan o puedan tener un impacto negativo en la integridad, la disponibilidad, la confidencialidad y/o la autenticidad de los servicios.
Alta dirección	(a) Para las entidades de crédito y las empresas de servicios de inversión, este término tiene el mismo significado que en la definición del artículo 3, apartado 1, punto 9, de la Directiva 2013/36/UE.

[2] Definición de las Directrices de la ABE sobre procedimientos y metodologías comunes para el proceso de revisión y evaluación supervisora de 19 de diciembre de 2014 (EBA/GL/2014/13), modificadas por EBA/GL/2018/03.

	(b) Para las entidades de pago y las entidades de dinero electrónico, este término significa las personas físicas que ejercen funciones ejecutivas en la entidad y que son responsables de la gestión diaria de la entidad y deben rendir cuentas de dicha gestión ante el órgano de dirección de la entidad. (c) Para los PSP mencionados en las letras c), e) y f) del artículo 1, apartado 1, de la Directiva (UE) 2015/2366, este término tiene el significado que le confiere la legislación nacional o la legislación de la Unión Europea aplicable.
Apetito de riesgo	Nivel agregado y tipos de riesgo que los PSP y entidades están dispuestos a asumir dentro de su capacidad de riesgo, en línea con su modelo de negocio, a fin de lograr sus objetivos estratégicos.
Función de auditoría	(a) Para las entidades de crédito y las empresas de servicios de inversión, la función de auditoría se define en la sección 22 de las Directrices de la ABE sobre gobierno interno (EBA/GL/2017/11). (b) Para los PSP distintos de las entidades de crédito, la función de auditoría debe ser independiente, tanto si está dentro del PSP como si es externa a él, pudiendo ser una función de auditoría interna y/o externa.
Proyectos de TIC	Cualquier proyecto, o parte del mismo, en el que se modifiquen, reemplacen, retiren o implementen sistemas y servicios de TIC. Los proyectos de TIC pueden ser parte de programas más amplios de TIC o de transformación del negocio.
Tercero	Organización que mantiene relaciones empresariales o contratos con una entidad para el suministro de un producto o servicio[3].
Activo de información	Recopilación de información, tangible o intangible, que merece protección.
Activo de TIC	Activo de software o hardware que se encuentra en el entorno de negocio.
Sistemas de TIC[4]	Configuración de los elementos de las TIC como parte de un mecanismo o una red de interconexión que sirve de soporte para las operaciones de una entidad financiera.
Servicios de TIC[5]	Servicios prestados por sistemas de TIC a uno o más usuarios internos o externos. Algunos ejemplos serían los servicios de entrada, almacenamiento y tratamiento de datos y los servicios de información, pero también los servicios de monitorización y de soporte al negocio y a la toma de decisiones.

[3] Definición de los elementos fundamentales del G7 para la gestión de riesgos cibernéticos de terceros en el sector financiero.
[4] Definición contenida en las Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES) (EBA/GL/ 2017/05).
[5] ibíd.

Aplicación

Fecha de aplicación

11. Estas directrices serán de aplicación a partir del 30 de junio de 2020.

Derogación

12. Las Directrices sobre las medidas de seguridad para los riesgos operativos y de seguridad (EBA/GL/2017/17) emitidas en 2017 serán derogadas por estas directrices en la fecha en que empiecen a ser aplicables.

Directrices sobre gestión de riesgos de TIC y de seguridad

1.1. Proporcionalidad

1. Todas las entidades financieras deberían cumplir las disposiciones establecidas en estas directrices de forma proporcional y acorde al tamaño de las entidades financieras y a su organización interna, así como a la naturaleza, el ámbito, la complejidad y el riesgo de los servicios y productos que suministran o tienen intención de suministrar.

1.2. Gobernanza y estrategia

1.2.1. Gobernanza

2. El órgano de dirección garantizará que las entidades financieras tengan un marco de gobierno interno y de control interno adecuado para sus riesgos de TIC y de seguridad. El órgano de dirección establecerá funciones y responsabilidades claras para las funciones de TIC, la gestión del riesgo de seguridad de la información y la continuidad del negocio, incluido también para el órgano de dirección y sus comités.
3. El órgano de dirección garantizará que la cantidad de personal de las entidades financieras y sus capacidades sean adecuadas para apoyar sus necesidades operativas de TIC y sus procesos de gestión de riesgos de TIC y de seguridad de manera continuada, así como para garantizar la aplicación de su estrategia de TIC. El órgano de dirección velará por que el presupuesto asignado sea adecuado para ello. Además, las entidades financieras se asegurarán de que todo su personal, incluidos los titulares de funciones clave, reciba formación adecuada en materia

de riesgos de TIC y de seguridad, incluida la seguridad de la información, con carácter anual o con mayor frecuencia si fuera necesario (véase también la sección 1.4.7.).

4. El órgano de dirección tiene la responsabilidad general de establecer, aprobar y supervisar la aplicación de la estrategia de TIC de las entidades financieras como parte de su estrategia general de negocio, así como de establecer un marco eficaz de gestión de riesgos de TIC y de seguridad.

1.2.2. Estrategia

5. La estrategia de TIC se ajustará a la estrategia general de negocio de las entidades financieras y definirá:
    a) cómo deben evolucionar las TIC de las entidades financieras para apoyar y participar con eficacia en su estrategia de negocio, incluida la evolución de la estructura organizativa, los cambios en los sistemas de TIC y las principales dependencias de terceros;
    b) la estrategia y evolución planificadas de la arquitectura de TIC, incluidas las dependencias de terceros;
    c) objetivos de seguridad de la información claros, centrados en los sistemas de TIC y los servicios, el personal y los procesos de TIC.
6. Las entidades financieras establecerán un conjunto de planes de acción con medidas que deben adoptarse para lograr el objetivo de la estrategia de TIC. Estos planes se comunicarán a todo el personal relevante (incluidos contratistas y proveedores cuando proceda y sea relevante). Los planes de acción se revisarán de forma periódica para garantizar que sean relevantes y apropiados. Las entidades financieras también establecerán procesos para realizar el seguimiento y medir la eficacia de la aplicación de su estrategia de TIC.

1.2.3. Uso de proveedores

7. Sin perjuicio de las Directrices de la ABE sobre acuerdos de externalización de servicios (EBA/GL/2019/02) y del artículo 19 de la DSP2, las entidades financieras velarán por la eficacia de las medidas de mitigación del riesgo definidas en su marco de gestión de riesgos, incluidas las medidas establecidas en estas directrices, cuando externalicen, incluso a entidades del grupo, las funciones operativas de los servicios de pago y/o los servicios y sistemas de TIC de cualquier actividad, o cuando recurran a terceros.
8. Para garantizar la continuidad de los servicios y sistemas de TIC, las entidades financieras garantizarán que los contratos y los acuerdos de nivel de servicio (tanto para circunstancias normales como en el caso de interrupciones del servicio, véase también la sección 1.7.2.) con proveedores (proveedores de servicios externalizados, entidades del grupo o proveedores externos) incluyan lo siguiente:
    a) objetivos y medidas relativos a la seguridad de la información apropiados y proporcionados, incluidos requisitos tales como requisitos mínimos en materia de ciberseguridad, especificaciones del ciclo de vida de los datos de la entidad financiera y

requisitos referentes a los procesos de cifrado de datos, seguridad de red y seguimiento de la seguridad, así como a la ubicación de los centros de datos;

b) procedimientos de gestión de incidentes de seguridad y operativos, incluidos los canales de comunicación y el escalado.

9. Las entidades financieras controlarán y obtendrán garantías del nivel de cumplimiento de los objetivos de seguridad, las medidas y los objetivos de rendimiento por parte de dichos proveedores.

1.3. Marco de gestión de riesgos de TIC y de seguridad

1.3.1. Organización y objetivos

10. Las entidades financieras identificarán y gestionarán sus riesgos de TIC y de seguridad. La función o funciones de TIC encargadas de los sistemas, procesos y operaciones de seguridad de TIC contarán con procesos y controles apropiados para garantizar que todos los riesgos se identifican, analizan, miden, vigilan, gestionan, comunican y mantienen dentro de los límites de apetito de riesgo de la entidad financiera y que sus proyectos y sistemas y las actividades que realizan cumplen los requisitos internos y externos.

11. Las entidades financieras asignarán la responsabilidad de gestión y supervisión de los riesgos de TIC y de seguridad a una función de control, en cumplimiento de los requisitos de la sección 19 de las Directrices de la ABE sobre gobierno interno (EBA/GL/2017/11). Asimismo, garantizarán la independencia y objetividad de esta función de control mediante su segregación adecuada de los procesos de las operaciones de TIC. Esta función de control rendirá cuentas directamente al órgano de dirección y será responsable de monitorizar y controlar el cumplimiento del marco de gestión de riesgos de TIC y de seguridad. Garantizará que los riesgos de TIC y de seguridad se identifican, miden, evalúan, gestionan, vigilan y comunican. Las entidades financieras se asegurarán de que esta función de control no sea responsable de ninguna auditoría interna.

    Utilizando un enfoque basado en el riesgo, la función de auditoría interna tendrá la capacidad de verificar de forma independiente y asegurar de forma objetiva que todas las actividades y unidades relacionadas con las TIC y la seguridad de la entidad financiera cumplen con las políticas y procedimientos internos y con los requisitos externos, satisfaciendo los requisitos de la sección 22 de las Directrices de la ABE sobre gobierno interno (EBA/GL/2017/11).

12. Las entidades financieras definirán y asignarán funciones y responsabilidades principales, así como los canales de comunicación pertinentes, para que el marco de gestión de riesgos de TIC y de seguridad sea eficaz. Este marco estará plenamente integrado en los procesos generales de gestión de riesgos de las entidades e irá en consonancia con ellos.

13. El marco de gestión de riesgos de TIC y de seguridad incluirá procesos establecidos para:

    a) determinar el apetito de riesgo de TIC y de seguridad, de conformidad con el apetito de riesgo de la entidad financiera;

b) identificar y evaluar los riesgos de TIC y de seguridad a los que la entidad financiera está expuesta;
c) definir medidas, incluidos controles, para mitigar los riesgos de TIC y de seguridad;
d) realizar un seguimiento de la eficacia de estas medidas, así como del número de incidentes comunicados, incluidos en el caso de los PSP los incidentes comunicados de conformidad con el artículo 96 de la DSP2 que afecten a las actividades relacionadas con las TIC, y actuar para corregir las medidas cuando sea necesario;
e) comunicar al órgano de dirección los riesgos de TIC y de seguridad y los controles correspondientes;
f) identificar y evaluar si existen riesgos de TIC y de seguridad derivados de cambios importantes en el sistema de TIC o en los servicios, procesos o procedimientos de TIC, y/o después de incidentes operativos o de seguridad importantes.

14. Las entidades financieras garantizarán que el marco de gestión de riesgos de TIC y de seguridad esté documentado y se mejore de forma continua, teniendo en cuenta la experiencia adquirida durante su aplicación y seguimiento. El órgano de dirección aprobará y revisará el marco de gestión de riesgos de TIC y de seguridad al menos una vez al año.

1.3.2. Identificación de funciones, procesos y activos

15. Las entidades financieras identificarán, establecerán y mantendrán actualizadas las relaciones entre las funciones de negocio, roles y procesos de apoyo para identificar la importancia de cada uno y sus interdependencias en cuanto a los riesgos de TIC y de seguridad.

16. Además, las entidades financieras identificarán, establecerán y mantendrán actualizadas las relaciones entre los activos de información que respaldan las funciones de negocio y los procesos de apoyo, tales como sistemas de TIC, personal, contratistas, terceros y dependencias de otros sistemas y procesos internos y externos, para poder, al menos, gestionar los activos de información que respaldan sus funciones y procesos de negocio críticos.

1.3.3. Clasificación y evaluación de riesgos

17. Las entidades financieras clasificarán las funciones de negocio, los procesos de apoyo y los activos de información identificados que se mencionan en los párrafos 15 y 16 en términos de criticidad.

18. Para definir la criticidad de estas funciones de negocio, procesos de apoyo y activos de información identificados, las entidades financieras tendrán en cuenta, como mínimo, los requisitos de confidencialidad, integridad y disponibilidad. La rendición de cuentas y la responsabilidad en relación con los activos de información estarán claramente asignadas.

19. Las entidades financieras revisarán la adecuación de la clasificación de los activos de información y documentación relevante cuando realicen la evaluación de riesgos.

20. Las entidades financieras identificarán los riesgos de TIC y de seguridad que impacten en las funciones de negocio, los procesos de apoyo y los activos de información identificados y clasificados de acuerdo con su criticidad. Esta evaluación de riesgos se realizará y documentará

anualmente o en intervalos más breves si es necesario. También se llevará a cabo cuando se produzcan cambios importantes en la infraestructura, los procesos o procedimientos que afecten a las funciones de negocio, los procesos de apoyo o los activos de información y que requieran por tanto que se actualice la evaluación de riesgos actual.

21. Las entidades financieras se asegurarán de realizar una monitorización continua de las amenazas y vulnerabilidades que afectan a sus procesos de negocio, funciones de apoyo y activos de información y revisarán periódicamente los escenarios de riesgo que tienen un impacto sobre ellos.

1.3.4. Mitigación de riesgos

22. Sobre la base de la evaluación de riesgos, las entidades financieras determinarán qué medidas se necesitan para mitigar hasta niveles aceptables los riesgos de TIC y de seguridad identificados y si son necesarios cambios en los procesos de negocio, las medidas de control y los sistemas y servicios de TIC existentes. Las entidades financieras considerarán el plazo necesario para aplicar estos cambios y el plazo para adoptar medidas de mitigación transitorias adecuadas para minimizar los riesgos de TIC y de seguridad con el objetivo de mantenerse dentro del nivel de apetito de riesgo de TIC y de seguridad que han establecido.

23. Las entidades financieras definirán y aplicarán medidas para mitigar los riesgos de TIC y de seguridad identificados y protegerán los activos de información de conformidad con su clasificación.

1.3.5. Comunicación

24. Las entidades financieras comunicarán los resultados de la evaluación de riesgos al órgano de dirección de manera clara y oportuna. Esta comunicación se realizará sin perjuicio de la obligación de los PSP de proporcionar a las autoridades competentes una evaluación de riesgos actualizada y completa, como se establece en el artículo 95, apartado 2, de la Directiva (UE) 2015/2366.

1.3.6. Auditoría

25. La gobernanza, los sistemas y los procesos relativos a los riesgos de TIC y de seguridad de las entidades financieras serán auditados de forma periódica por auditores con suficientes conocimientos, competencias y experiencia en riesgos de TIC y de seguridad y en pagos (para los PSP) para ofrecer una garantía independiente de su eficacia al órgano de dirección. Los auditores serán independientes tanto si pertenecen a la entidad financiera como si son ajenos a ella. La frecuencia y el enfoque de estas auditorías serán adecuados a los riesgos de TIC y de seguridad pertinentes.

26. El órgano de dirección de las entidades financieras aprobará el plan de auditoría, incluidas las auditorías de TIC, y cualquier modificación importante del mismo. El plan de auditoría y su ejecución, incluida la frecuencia de auditoría, deberán reflejar y ser proporcionales a los riesgos de TIC y de seguridad inherentes a la entidad financiera y se actualizarán con regularidad.

27. Debe establecerse un proceso formal de seguimiento que incluya disposiciones para la verificación y corrección oportunas de las deficiencias críticas halladas en las auditorías de TIC.

1.4. Seguridad de la información

1.4.1. Política de seguridad de la información

28. Las entidades financieras elaborarán y documentarán una política de seguridad de la información que debería definir los principios y normas de alto nivel para proteger la confidencialidad, integridad y disponibilidad de los datos y la información de las entidades financieras y sus clientes. Para los PSP, esta política se identifica en el documento de política de seguridad que debe adoptarse de conformidad con el artículo 5, apartado 1, letra j), de la Directiva (UE) 2015/2366. La política de seguridad de la información será acorde a los objetivos de seguridad de la información de la entidad financiera y se basará en los resultados relevantes del proceso de evaluación de riesgos. La política será adoptada por el órgano de dirección.

29. La política incluirá una descripción de las principales funciones y responsabilidades de la gestión de la seguridad de la información, y establecerá los requisitos que deben cumplir el personal y los contratistas, los procesos y la tecnología en relación con la seguridad de la información, reconociendo que el personal y los contratistas a todos niveles tienen responsabilidades a la hora de garantizar la seguridad de la información de la entidad financiera. La política garantizará la confidencialidad, la integridad y la disponibilidad de los activos lógicos y físicos, los recursos y los datos sensibles críticos de la entidad financiera, tanto si están en reposo como si están en tránsito o en uso. La política de seguridad de la información se comunicará a todo el personal y a todos los contratistas de la entidad financiera.

30. Sobre la base de la política de seguridad de la información, las entidades financieras establecerán y aplicarán medidas de seguridad destinadas a mitigar los riesgos de TIC y de seguridad a los que están expuestas. Estas medidas incluirán:

    a) organización y gobernanza de conformidad con los párrafos 10 y 11;
    b) seguridad lógica (sección 1.4.2.);
    c) seguridad física (sección 1.4.3.);
    d) seguridad de las operaciones de TIC (sección 1.4.4.);
    e) seguimiento de la seguridad (sección 1.4.5.);
    f) revisiones, evaluaciones y pruebas de la seguridad de la información (sección 1.4.6.);
    g) formación y concienciación sobre seguridad de la información (sección 1.4.7.).

1.4.2. Seguridad lógica

31. Las entidades financieras definirán, documentarán e implementarán procedimientos para el control de acceso lógico (gestión de identidades y accesos). Estos procedimientos se implantarán, aplicarán, vigilarán y revisarán de forma periódica. También incluirán controles para realizar un seguimiento de anomalías. Estos procedimientos contendrán, como mínimo, los siguientes elementos, en los que el término «usuario» también incluye a los usuarios técnicos:

(a) Necesidad de conocer, mínimo privilegio y segregación de funciones: las entidades financieras gestionarán los derechos de acceso a los activos de información y sus sistemas de apoyo según el principio de «necesidad de conocer», también para el acceso remoto. A los usuarios se les concederán los mínimos derechos de acceso que sean estrictamente necesarios para ejercer sus funciones (principio del «mínimo privilegio»), a fin de evitar el acceso no justificado a un conjunto amplio de datos o evitar la asignación de combinaciones de derechos de acceso que puedan ser utilizadas para eludir los controles (principio de «segregación de funciones»).

(b) Responsabilidad de los usuarios: las entidades financieras limitarán, en la medida de lo posible, el uso de cuentas de usuario genéricas y compartidas y garantizarán que se pueda identificar a los usuarios que ejecutan acciones en los sistemas de TIC.

(c) Derechos de acceso privilegiado: las entidades financieras aplicarán controles sólidos sobre el acceso privilegiado a los sistemas mediante la limitación estricta y supervisión estrecha de las cuentas con elevados derechos de acceso a los sistemas (por ejemplo, cuentas de administrador). Con el fin de garantizar una comunicación segura y reducir el riesgo, el acceso administrativo remoto a sistemas de TIC críticos solo se concederá según el principio de «necesidad de conocer» y en caso de que se usen soluciones de autenticación fuerte.

(d) Registro de actividad de los usuarios: como mínimo, se registrarán y monitorizarán todas las actividades de los usuarios privilegiados. Los registros de acceso se protegerán para evitar modificaciones o borrados no autorizados y se conservarán durante un periodo acorde con la criticidad de las funciones de negocio, los procesos de apoyo y los activos de información identificados, conforme a la sección 1.1.3., sin perjuicio de los requisitos de conservación estipulados en la legislación nacional y de la Unión Europea. Las entidades financieras usarán dicha información para facilitar la identificación y la investigación de actividades anómalas que se hayan detectado en la prestación de los servicios.

(e) Gestión de accesos: los derechos de acceso se concederán, retirarán o modificarán de manera oportuna, de acuerdo con los flujos de aprobación predefinidos en los que participa el propietario de la información a la que se accede (propietario del activo de información). En caso de cese de la relación laboral, los derechos de acceso se retirarán inmediatamente.

(f) Recertificación de accesos: los derechos de acceso se revisarán periódicamente para garantizar que los usuarios no poseen privilegios excesivos y que los derechos de acceso se retiran cuando ya no son necesarios.

(g) Métodos de autenticación: las entidades financieras aplicarán métodos de autenticación suficientemente robustos para garantizar de forma adecuada y eficaz el cumplimiento de las políticas y los procedimientos de control de acceso. Los métodos de autenticación serán adecuados a la criticidad de los sistemas de TIC, la información o el proceso a los que se accede. Deben incluir, como mínimo, contraseñas complejas o métodos de autenticación más fuerte (como la autenticación de doble factor), en función del riesgo pertinente.

32. El acceso electrónico mediante aplicaciones a los datos y sistemas de TIC se limitará al mínimo imprescindible para prestar el servicio correspondiente.

1.4.3. Seguridad física

33. Las entidades financieras definirán, documentarán y aplicarán medidas de seguridad física para proteger sus instalaciones, centros de datos y zonas sensibles frente a accesos no autorizados y a peligros ambientales.

34. El acceso físico a los sistemas TIC se permitirá únicamente a las personas autorizadas. La autorización se asignará conforme a las tareas y responsabilidades de la persona y se limitará a aquellas personas que cuentan con la formación y la supervisión adecuadas. El acceso físico se revisará con regularidad para asegurar que los derechos de acceso innecesarios se revocan en cuanto dejan de ser necesarios.

35. Las medidas adecuadas para proteger de peligros ambientales serán acordes a la importancia de los edificios y la criticidad de las operaciones o sistemas de TIC ubicados en ellos.

1.4.4. Seguridad de las operaciones de TIC

36. Las entidades financieras pondrán en marcha procedimientos para evitar problemas de seguridad en los sistemas y servicios de TIC y minimizarán su efecto en la prestación de los servicios de TIC. Estos procedimientos incluirán las siguientes medidas:

    a) identificación de vulnerabilidades potenciales, que deben evaluarse y corregirse garantizando que el software y el firmware estén actualizados, incluido el software proporcionado por las entidades financieras a sus usuarios internos y externos, aplicando parches de seguridad críticos o implementando controles compensatorios;
    b) aplicación de líneas base de configuración segura de todos los componentes de red;
    c) segmentación de redes, sistemas de prevención de pérdida de datos y cifrado del tráfico de red (de conformidad con la clasificación de los datos);
    d) protección de equipos, incluidos servidores, estaciones de trabajo y dispositivos móviles; las entidades financieras deben evaluar si los equipos cumplen los estándares de seguridad definidos por ellas antes de otorgar acceso a la red corporativa;
    e) garantizar que existen mecanismos para verificar la integridad del software, el firmware y los datos;
    f) cifrado de datos en reposo y en tránsito (de conformidad con la clasificación de los datos).

37. Además, de manera continuada, las entidades financieras determinarán si los cambios en el entorno operativo existente influyen en las medidas de seguridad actuales o requieren la adopción de medidas adicionales para mitigar adecuadamente los riesgos relacionados. Dichos cambios serán parte del proceso formal de gestión de cambios de las entidades financieras que debería garantizar la adecuada planificación, prueba, documentación, autorización e implementación de estos cambios.

1.4.5. Monitorización de la seguridad

38. Las entidades financieras establecerán y aplicarán políticas y procedimientos para detectar actividades anómalas que puedan afectar a la seguridad de su información y responder a estos eventos de manera adecuada. Como parte de esta monitorización continua, las entidades financieras establecerán capacidades eficaces y adecuadas para detectar y comunicar intrusiones físicas o lógicas, así como violaciones de la confidencialidad, la integridad y la disponibilidad de los activos de información. Los procesos de monitorización y detección continuos abarcarán lo siguiente:

    a) factores internos y externos relevantes, incluidas las funciones administrativas de TIC y del negocio;
    b) operaciones para detectar el uso indebido del acceso por parte de terceros y otras entidades, así como el acceso indebido interno;
    c) amenazas potenciales internas y externas.

39. Las entidades financieras establecerán e implantarán procesos y estructuras organizativas para identificar y realizar un seguimiento constante de las amenazas de seguridad que podrían afectar de manera importante a su capacidad para prestar servicios. Realizarán un seguimiento activo de los avances tecnológicos para asegurar que conocen los riesgos de seguridad. Las entidades financieras implantarán medidas de detección, por ejemplo, para identificar posibles filtraciones de información, código malicioso y otras amenazas de seguridad y vulnerabilidades de dominio público en el software y el hardware. Asimismo, deben comprobar las nuevas actualizaciones de seguridad que correspondan.

40. El proceso de monitorización de la seguridad también debe ayudar a la entidad financiera a entender la naturaleza de los incidentes operativos o de seguridad, identificar las tendencias y apoyar las investigaciones de la organización.

1.4.6. Revisiones, evaluaciones y pruebas de la seguridad de la información

41. Las entidades financieras realizarán diversas revisiones, evaluaciones y pruebas de la seguridad de la información para garantizar la identificación eficaz de las vulnerabilidades de sus sistemas y servicios de TIC. Por ejemplo, pueden realizar análisis de gaps con respecto a los estándares de seguridad de la información, revisiones del cumplimiento, auditorías internas y externas de los sistemas de información o revisiones de la seguridad física. Además, las entidades considerarán la introducción de buenas prácticas como revisiones del código fuente, evaluaciones de vulnerabilidad, pruebas de penetración y ejercicios de red team.

42. Las entidades financieras establecerán y aplicarán un marco de pruebas de la seguridad de la información que valide la solidez y la eficacia de sus medidas de seguridad de la información y garantizarán que este marco considere las amenazas y vulnerabilidades identificadas mediante el seguimiento de amenazas y el proceso de evaluación de riesgos de TIC y de seguridad.

43. El marco de pruebas de la seguridad de la información garantizará que las pruebas:

a) sean realizadas por evaluadores independientes con conocimientos, competencias y experiencia suficientes en pruebas de medidas de seguridad de la información, que no hayan participado en la elaboración de dichas medidas;
b) incluyan exploraciones sistemáticas de vulnerabilidades y pruebas de penetración (incluidas pruebas de tipo threat-led penetration testing cuando sea necesario y apropiado) proporcionales al nivel del riesgo identificado en los procesos de negocio y sistemas.

44. Las entidades financieras realizarán pruebas continuas y repetidas de las medidas de seguridad. Para todos los sistemas críticos de TIC (párrafo 17), estas pruebas se llevarán a cabo al menos anualmente y, para los PSP, formarán parte de la evaluación completa de los riesgos de seguridad relacionados con los servicios de pago que prestan, de conformidad con el artículo 95, apartado 2, de la DSP2. Los sistemas no críticos se probarán de manera periódica según un enfoque basado en el riesgo, pero al menos una vez cada tres años.

45. Las entidades financieras garantizarán que se prueben las medidas de seguridad en el caso de cambios en la infraestructura, los procesos o los procedimientos y también si se realizan cambios derivados de importantes incidentes operativos o de seguridad o debido al lanzamiento de aplicaciones críticas publicadas en Internet nuevas o con modificaciones significativas.

46. Las entidades financieras monitorizarán y evaluarán los resultados de las pruebas de seguridad y actualizarán sus medidas de seguridad en consecuencia y sin demoras injustificadas en el caso de los sistemas críticos de TIC.

47. Para los PSP, el marco de pruebas también abarcará las medidas de seguridad correspondientes a: 1) los terminales y dispositivos de pago usados para la prestación de servicios de pago, 2) los terminales y dispositivos de pago usados para la autenticación de los usuarios de servicios de pago; y 3) los dispositivos y el software proporcionados por el PSP al usuario de servicios de pago para generar o recibir un código de autenticación.

48. Sobre la base de las amenazas de seguridad observadas y de las modificaciones realizadas, se realizarán las pruebas oportunas para incorporar escenarios de posibles ataques relevantes y conocidos.

1.4.7. Formación y concienciación sobre seguridad de la información

49. Las entidades financieras establecerán un programa de formación, incluidos programas periódicos de concienciación sobre seguridad, para la totalidad del personal y los contratistas a fin de asegurarse de que cuentan con la formación necesaria para cumplir sus funciones y responsabilidades conforme a las políticas y procedimientos de seguridad oportunos y reducir errores humanos, robos, fraudes, usos indebidos o pérdidas y saber cómo abordar los riesgos relacionados con la seguridad de la información. Las entidades financieras garantizarán que el programa de formación ofrezca formación a todo el personal y a los contratistas al menos anualmente.

1.5. Gestión de las operaciones de TIC

50. Las entidades financieras gestionarán sus operaciones de TIC sobre la base de los procesos y procedimientos documentados e implementados (que, en el caso de los PSP, incluye el documento de política de seguridad de conformidad con el artículo 5, apartado 1, letra j), de la DSP2) que han sido aprobados por el órgano de dirección. Este conjunto de documentos definirá cómo las entidades financieras operan, monitorizan y controlan sus sistemas y servicios de TIC, incluida la documentación de operaciones críticas de TIC, y permitirá a las entidades financieras mantener un inventario actualizado de activos de TIC.

51. Las entidades financieras garantizarán que el rendimiento de sus operaciones de TIC se ajusta a las necesidades de su negocio. Deben mantener y mejorar, cuando sea posible, la eficiencia de sus operaciones de TIC, considerando, entre otras cosas, cómo minimizar errores potenciales derivados de la ejecución de tareas manuales.

52. Las entidades financieras aplicarán procedimientos de registro y monitorización de las operaciones críticas de TIC con el objetivo de detectar, analizar y corregir errores.

53. Las entidades financieras mantendrán un inventario actualizado de sus activos de TIC (incluidos sistemas de TIC, dispositivos de red, bases de datos, etc.). El inventario de activos de TIC deberá almacenar la configuración de los activos de TIC y los vínculos e interdependencias entre los distintos activos de TIC, para permitir un proceso adecuado de configuración y gestión de cambios.

54. El inventario de activos de TIC será suficientemente detallado para permitir la identificación inmediata de un activo de TIC, su ubicación, clasificación de seguridad y propietario. Se documentarán las interdependencias entre los activos para ayudar en la respuesta a incidentes operativos y de seguridad, incluidos ciberataques.

55. Las entidades financieras monitorizarán y gestionarán los ciclos de vida de los activos de TIC, para garantizar que continúan cumpliendo y respaldando las necesidades del negocio y de la gestión de riesgos. Las entidades financieras vigilarán si sus proveedores y desarrolladores externos o internos dan soporte a sus activos de TIC y si todos los parches y actualizaciones relevantes se aplican sobre la base de procesos documentados. Deberán evaluarse y mitigarse los riesgos derivados de activos de TIC obsoletos o sin soporte.

56. Las entidades financieras deben aplicar procesos de planificación y seguimiento de la capacidad y el rendimiento para prevenir, detectar y responder oportunamente a problemas importantes de rendimiento de los sistemas de TIC y a la falta de capacidad de TIC.

57. Las entidades financieras definirán y aplicarán procedimientos de copia de seguridad y restauración de datos y sistemas de TIC para garantizar que puedan recuperarse cuando sea preciso. El alcance y la frecuencia de las copias de seguridad se establecerán conforme a las necesidades de recuperación del negocio y la criticidad de los datos y los sistemas de TIC y se evaluarán según la evaluación de riesgos realizada. Los procedimientos de copias de seguridad y restauración se someterán a pruebas periódicas.

58. Las entidades financieras deben garantizar que las copias de seguridad de datos y sistemas de TIC se almacenen de forma segura y en un lugar suficientemente alejado de la ubicación principal para que no estén expuestos a los mismos riesgos.

1.5.1 Gestión de incidentes y problemas de TIC

59. Las entidades financieras establecerán y aplicarán un proceso de gestión de incidentes y problemas para monitorizar y registrar los incidentes operativos y de seguridad de TIC y para permitir que las entidades financieras continúen o restablezcan, de manera oportuna, funciones y procesos de negocio críticos cuando se producen interrupciones. Las entidades financieras determinarán los criterios y umbrales adecuados para clasificar los sucesos como incidentes operativos o de seguridad, tal como se establece en la sección de «Definiciones» de estas directrices, así como los indicadores de alerta temprana que deben servir como avisos para permitir una detección temprana de estos incidentes. Estos criterios y umbrales, para los PSP, son sin perjuicio de la clasificación de los incidentes graves de conformidad con el artículo 96 de la DSP2 y las Directrices sobre la notificación de incidentes graves de conformidad con la DSP2 (EBA/GL/2017/10).

60. Para minimizar el efecto de acontecimientos adversos y permitir una recuperación oportuna, las entidades financieras establecerán procesos y estructuras organizativas apropiados que garanticen un control, tratamiento y seguimiento integrados y coherentes de los incidentes operativos y de seguridad y que aseguren que se identifican y eliminan las causas de fondo para evitar que se repitan los incidentes. El proceso de gestión de incidentes y problemas establecerá:

    a) Los procedimientos para identificar, seguir, registrar, categorizar y clasificar los incidentes según una prioridad, en función de la criticidad para el negocio;
    b) las funciones y responsabilidades en los distintos escenarios de incidentes (por ejemplo, errores, fallos en el funcionamiento, ciberataques, etc.);
    c) procedimientos de gestión de problemas para identificar, analizar y resolver las causas de fondo de uno o más incidentes; las entidades financieras analizarán los incidentes operativos o de seguridad que pudieran afectarles que hayan sido identificados o se hayan producido dentro y/o fuera de la organización y considerarán las principales lecciones aprendidas de estos análisis y actualizarán las medidas de seguridad en consecuencia;
    d) planes de comunicación interna eficaz, incluidos procedimientos de comunicación y escalado de incidentes, que también abarquen las reclamaciones de los clientes relacionadas con la seguridad, para velar por que:
        i) los incidentes con un efecto adverso potencialmente elevado sobre sistemas y servicios de TIC críticos sean comunicados a la alta dirección pertinente y a la alta dirección de TIC;
        ii) se informe al órgano de dirección de manera ad hoc en el caso de incidentes significativos y, a menos, del efecto, la respuesta y los controles adicionales que deben definirse como resultado de los incidentes.

e) procedimientos de respuesta a incidentes para mitigar sus efectos y garantizar que el servicio vuelva a estar operativo y sea seguro lo antes posible;
f) planes específicos de comunicación externa para funciones y procesos de negocio críticos con el objetivo de:
    i) colaborar con partes interesadas relevantes para responder con eficacia y recuperarse del incidente;
    ii) ofrecer información oportuna a actores externos (por ejemplo, clientes, otros participantes del mercado, la autoridad de supervisión, etc.) según corresponda y de conformidad con la normativa aplicable.

1.6. Gestión de proyectos y de cambios de TIC

1.6.1. Gestión de proyectos de TIC

61. Las entidades financieras aplicarán un programa y/o un proceso de gobernanza de proyectos que defina funciones, obligaciones y responsabilidades para respaldar eficazmente la aplicación de la estrategia de TIC.

62. Las entidades financieras realizarán un seguimiento apropiado y mitigarán los riesgos derivados de su cartera de proyectos de TIC (gestión de programas), considerando también los riesgos que puedan resultar de las interdependencias entre proyectos distintos y de la dependencia de múltiples proyectos de los mismos recursos o conocimientos técnicos.

63. Las entidades financieras establecerán y aplicarán una política de gestión de proyectos de TIC que incluya, como mínimo:

    a) objetivos del proyecto;

    b) funciones y responsabilidades;

    c) una evaluación del riesgo del proyecto;

    d) un plan, un calendario y las fases del proyecto;

    e) principales hitos;

    f) requisitos de gestión del cambio.

64. La política de gestión de proyectos de TIC garantizará que los requisitos en materia de seguridad de la información son analizados y aprobados por una función independiente de la función de desarrollo.

65. Las entidades financieras velarán por que todas las áreas afectadas por un proyecto de TIC estén representadas en el equipo del proyecto y que este equipo cuente con los conocimientos necesarios para garantizar que el proyecto pueda implementarse de forma segura y con éxito.

66. El establecimiento y el avance de los proyectos de TIC y sus riesgos asociados se notificarán al órgano de dirección, de forma individual o conjunta, dependiendo de la importancia y el tamaño de dichos proyectos, con carácter periódico o ad hoc, según corresponda. Las entidades

financieras incluirán los riesgos derivados de su cartera de proyectos en su marco de gestión de riesgos.

1.6.2. Adquisición y desarrollo de sistemas de TIC

67. Las entidades financieras desarrollarán y aplicarán un proceso que rija la adquisición, el desarrollo y el mantenimiento de los sistemas de TIC. Este proceso se diseñará según un enfoque basado en el riesgo.

68. Las entidades financieras garantizarán que, antes de que se adquieran o desarrollen sistemas de TIC, los requisitos funcionales y no funcionales (incluidos los requisitos en materia de seguridad de la información) estén claramente definidos y aprobados por la dirección del área correspondiente.

69. Las entidades financieras garantizarán que se han implantado medidas para mitigar el riesgo de alteración no intencionada o manipulación intencionada de los sistemas de TIC durante el desarrollo y la implementación en el entorno de producción.

70. Las entidades financieras contarán con una metodología para la realización de pruebas y la aprobación de los sistemas de TIC antes de utilizarlos por primera vez. Esta metodología considerará la criticidad de los procesos y activos de negocio. Las pruebas garantizarán que los nuevos sistemas de TIC funcionen del modo previsto. También utilizarán entornos de prueba que reflejen adecuadamente el entorno de producción.

71. Las entidades financieras probarán los sistemas de TIC, los servicios de TIC y las medidas de seguridad de la información para identificar posibles debilidades, violaciones e incidentes de seguridad.

72. Las entidades financieras implementarán entornos de TIC separados para garantizar una adecuada segregación de funciones y mitigar el efecto de cambios no verificados en los sistemas de producción. En concreto, deben garantizar que los entornos de producción estén segregados de los entornos de desarrollo, pruebas y otros entornos que no son de producción. Las entidades financieras garantizarán la integridad y confidencialidad de los datos de producción en los entornos que no son de producción. El acceso a datos de producción está restringido a los usuarios autorizados.

73. Las entidades financieras aplicarán medidas para proteger la integridad de los códigos fuente de sistemas de TIC que se desarrollan internamente. También documentarán el desarrollo, la aplicación, la operación y la configuración de los sistemas de TIC de manera exhaustiva para reducir cualquier dependencia innecesaria de expertos en la materia. La documentación de los sistemas de TIC contendrá, cuando proceda, al menos documentación de usuario, documentación técnica del sistema y procedimientos operativos.

74. Los procesos de adquisición y desarrollo de sistemas de TIC de la entidad financiera también deben aplicarse a los sistemas de TIC desarrollados o gestionados por los usuarios finales de las funciones de negocio que no pertenecen a la organización de TIC (por ejemplo, aplicaciones informáticas de usuario final) según un enfoque basado en el riesgo. Las entidades financieras

mantendrán un registro de estas aplicaciones que dan soporte a funciones de negocio o procesos críticos.

1.6.3. Gestión de cambios de TIC

75. Las entidades financieras establecerán y aplicarán un proceso de gestión de cambios de TIC para garantizar que todos los cambios en los sistemas de TIC se registren, prueben, evalúen, aprueben, apliquen y verifiquen de forma controlada. Las entidades financieras gestionarán los cambios urgentes (es decir, los cambios que deben introducirse lo antes posible) siguiendo procedimientos que ofrezcan garantías adecuadas.

76. Las entidades financieras determinarán si los cambios en el entorno operativo existente influyen en las medidas de seguridad actuales o requieren la adopción de medidas adicionales para mitigar los riesgos que conllevan. Estos cambios serán conformes con el proceso formal de gestión de cambios de las entidades financieras.

1.7. Gestión de la continuidad del negocio

77. Las entidades financieras establecerán un proceso adecuado de gestión de la continuidad del negocio con el fin de maximizar su capacidad para prestar servicios de forma continuada y limitar las pérdidas en caso de interrupciones graves de la actividad, de conformidad con el artículo 85, apartado 2, de la Directiva 2013/36/UE y el Título VI de las Directrices de la ABE sobre gobierno interno (EBA/GL/2017/11).

1.7.1. Análisis de impacto en el negocio

78. Como parte de una gestión adecuada de la continuidad del negocio, las entidades financieras llevarán a cabo análisis de impacto en el negocio mediante el análisis de su exposición a interrupciones graves de la actividad y la evaluación de los impactos potenciales (incluido sobre la confidencialidad, la integridad y la disponibilidad), en términos cuantitativos y cualitativos, utilizando datos internos y externos (por ejemplo, datos de un proveedor externo relevantes para un proceso de negocio o datos disponibles públicamente que puedan ser relevantes para el análisis de impacto en el negocio) y el análisis de escenarios. El análisis de impacto en el negocio también considerará la criticidad de las funciones de negocio, los procesos de apoyo, los terceros implicados y los activos de información identificados y clasificados, así como sus interdependencias, de conformidad con la sección 1.1.3.

79. Las entidades financieras garantizarán que sus sistemas y servicios de TIC estén diseñados en consonancia con su análisis de impacto en el negocio, por ejemplo, con redundancia de ciertos componentes críticos para evitar interrupciones causadas por eventos que afecten a esos componentes.

1.7.2. Planificación de la continuidad del negocio

80. Sobre la base de sus análisis de impacto en el negocio, las entidades financieras establecerán planes para asegurar la continuidad del negocio (planes de continuidad del negocio), que se

documentarán y serán aprobados por los órganos de dirección. Los planes considerarán en concreto los riesgos que podrían tener un impacto adverso en los sistemas y servicios de TIC. Los planes servirán de apoyo a los objetivos de protección y, si fuera necesario, de restablecimiento de la confidencialidad, integridad y disponibilidad de sus funciones de negocio, procesos de apoyo y activos de información. Las entidades financieras se coordinarán con las partes implicadas que corresponda, internas y externas, durante el establecimiento de estos planes.

81. Las entidades financieras establecerán planes de continuidad del negocio para asegurar que pueden reaccionar adecuadamente ante posibles escenarios de fallo y que son capaces de recuperar las operaciones de sus actividades de negocio críticas después de interrupciones de la actividad cumpliendo un objetivo de tiempo de recuperación (RTO, el tiempo máximo en el que un sistema o proceso debe ser restaurado después de un incidente) y un objetivo de punto de recuperación (RPO, el periodo de tiempo máximo en el que es aceptable la pérdida de datos en caso de que se produzca un incidente). En casos de interrupciones graves de la actividad que activan planes específicos de continuidad del negocio, las entidades financieras priorizarán las acciones de continuidad del negocio mediante un enfoque basado en el riesgo, que puede basarse en las evaluaciones de riesgos realizadas de conformidad con la sección 1.1.3. Para los PSP esto puede incluir, por ejemplo, facilitar que continúe el procesamiento de las operaciones críticas mientras duren las medidas de recuperación.

82. Las entidades financieras considerarán varios escenarios diferentes en su plan de continuidad del negocio que incluirán escenarios extremos pero plausibles a los que podrían estar expuestas, incluido un escenario de ciberataque, y evaluarán su posible impacto. Sobre la base de estos escenarios, las entidades financieras describirán cómo se garantizan la continuidad de sus sistemas y servicios de TIC y la seguridad de su información.

1.7.3. Planes de respuesta y recuperación

83. Sobre la base de los análisis de impacto en el negocio (párrafo 78) y los escenarios plausibles (párrafo 82), las entidades financieras elaborarán planes de respuesta y recuperación. Estos planes especificarán qué condiciones pueden provocar su activación y qué acciones deben adoptarse para garantizar la disponibilidad, continuidad y recuperación de, al menos, los servicios y sistemas de TIC críticos de las entidades financieras. Los planes de respuesta y recuperación tendrán como objetivo cumplir los objetivos de recuperación de las operaciones de las entidades financieras.

84. Los planes de respuesta y recuperación considerarán opciones de recuperación tanto a corto como a largo plazo. Estos planes:

    a) se centrarán en la recuperación de las operaciones de las funciones de negocio, procesos de apoyo y activos de información críticos y sus interdependencias para evitar efectos adversos en el funcionamiento de las entidades financieras y en el sistema financiero, incluidos los sistemas de pago y los usuarios de servicios de pago, y garantizar la ejecución de las operaciones de pago pendientes;

b) estarán documentados y a disposición de las unidades de negocio y de apoyo y serán fácilmente accesibles en caso de emergencia;
c) estarán actualizados teniendo en cuenta las lecciones aprendidas durante los incidentes, las pruebas, los nuevos riesgos identificados, las amenazas y los cambios en los objetivos y prioridades de recuperación.

85. Los planes también considerarán opciones alternativas cuando no sea posible la recuperación en el corto plazo debido a los costes, los riesgos, la logística o circunstancias imprevistas.

86. Además, como parte de los planes de respuesta y recuperación, las entidades financieras considerarán y aplicarán medidas de continuidad para mitigar fallos de proveedores externos, que son fundamentales para la continuidad de su servicio de TIC (de conformidad con las disposiciones de las Directrices de la ABE sobre acuerdos de externalización de servicios (EBA/GL/2019/02) en relación con los planes de continuidad de negocio).

1.7.4. Pruebas de los planes

87. Las entidades financieras probarán sus planes de continuidad del negocio de forma periódica. En particular, se asegurarán de que los planes de continuidad del negocio de sus funciones de negocio, procesos de apoyo y activos de información críticos y sus interdependencias (incluidos los prestados por terceros, cuando proceda) se sometan a pruebas al menos una vez al año, de conformidad con el párrafo 89.

88. Los planes de continuidad del negocio se actualizarán al menos una vez al año, en función de los resultados de las pruebas, la información sobre amenazas actuales y las lecciones aprendidas de eventos anteriores. Los cambios en los objetivos de recuperación (incluidos los objetivos de tiempo de recuperación y los objetivos de punto de recuperación) y los cambios en las funciones de negocio, los procesos de apoyo y los activos de información también se utilizarán de base, en su caso, para actualizar los planes de continuidad del negocio.

89. Las pruebas que realizan las entidades financieras a sus planes de continuidad del negocio deben demostrar que son capaces de sostener la viabilidad de su negocio hasta que se restablezcan las operaciones críticas. En particular:

a) incluirán pruebas de un conjunto adecuado de escenarios graves pero plausibles, incluidos aquellos considerados para la elaboración de los planes de continuidad del negocio (así como pruebas de los servicios prestados por terceros, cuando corresponda), entre ellos el traspaso de funciones de negocio, procesos de apoyo y activos de información críticos al entorno de recuperación frente a desastres y la demostración de que pueden funcionar de esta forma durante un periodo de tiempo suficientemente representativo y que posteriormente puede restaurarse el funcionamiento normal;
b) estarán diseñadas para poner en cuestión los supuestos en los que se basan los planes de continuidad del negocio, incluidos los planes de comunicación de crisis y los procedimientos de gobierno interno; e

c) incluirán procedimientos para verificar la capacidad de su personal y los contratistas, los sistemas de TIC y los servicios de TIC para responder adecuadamente a los escenarios definidos en el párrafo 89, letra a).

90. Los resultados de las pruebas se documentarán y las deficiencias identificadas como resultado de las pruebas se analizarán, abordarán y comunicarán al órgano de dirección.

1.7.5. Comunicación de crisis

91. En el caso de que ocurra una interrupción o una emergencia, y durante la implantación de los planes de continuidad del negocio, las entidades financieras se asegurarán de que disponen de medidas eficaces de comunicación de crisis que permitan que todas las partes implicadas, internas y externas, incluidas las autoridades competentes cuando así lo requieran las normativas nacionales, y también los proveedores pertinentes (proveedores de servicios externalizados, entidades del grupo o proveedores externos), sean informadas de manera oportuna y adecuada.

1.8. Gestión de la relación con los usuarios de servicios de pago

92. Los PSP establecerán e implantarán procesos para mejorar la concienciación de los usuarios de servicios de pago en cuanto a los riesgos de seguridad asociados con los servicios de pago proporcionando asistencia y orientación a dichos usuarios.

93. La asistencia y orientación ofrecida a los usuarios de servicios de pago se actualizará a la luz de nuevas amenazas o vulnerabilidades y los cambios se comunicarán a dichos usuarios.

94. Cuando la funcionalidad del producto lo permita, los PSP permitirán a los usuarios de servicios de pago desactivar funcionalidades concretas relacionadas con los servicios de pago que ofrecen a dichos usuarios.

95. En los casos en que, con arreglo al apartado 1 del artículo 68 de la Directiva (UE) 2015/2366, un PSP acuerde con el ordenante un límite de gasto aplicable a las operaciones de pago ejecutadas mediante instrumentos de pago específicos, el PSP proporcionará al ordenante la opción de ajustar dichos límites hasta el límite máximo acordado.

96. Los PSP ofrecerán a los usuarios de servicios de pago la opción de recibir alertas sobre las operaciones de pago iniciadas y sobre los intentos fallidos de iniciarlas para permitirles detectar el uso fraudulento o malicioso de su cuenta.

97. Los PSP mantendrán informados a los usuarios de servicios de pago sobre las actualizaciones de los procedimientos de seguridad que afecten a dichos usuarios en relación con la prestación de servicios de pago.

98. Los PSP proporcionarán asistencia a los usuarios de servicios de pago ante cualquier pregunta, solicitud de ayuda y notificación de anomalías o problemas relacionados con cuestiones de seguridad de los servicios de pago. Los usuarios de servicios de pago deberán ser debidamente informados sobre cómo pueden obtener dicha asistencia.