EBA/GL/2017/17

12/01/2018

Directrices

sobre las medidas de seguridad para los riesgos operativos y de seguridad asociados a los servicios de pago en virtud de la Directiva (UE) 2015/2366 (PSD2)

1. 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) nº 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 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 en un determinado ámbito. Las autoridades competentes definidas en el artículo 4, apartado 2, del Reglamento (UE) nº 1093/2010 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) nº 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el 12.03.2018, si cumplen o se proponen cumplir estas directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho 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/2017/17». Las notificaciones serán presentadas 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 y como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) nº 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 nº 716/2009/CE y se deroga la Decisión nº 2009/78/CE de la Comisión, (DO L 331 de 15.12.2010, p. 12).

2. Objeto, ámbito de aplicación y definiciones

Objeto y ámbito de aplicación

5. Estas Directrices se derivan del mandato otorgado a la EBA en el artículo 95, apartado 3 de la Directiva (UE) 2015/2366[2] (PSD2).

6. Estas Directrices especifican los requisitos para el establecimiento, la aplicación y el seguimiento de las medidas de seguridad que deben adoptar los PSP (proveedores de servicios de pago), conforme al apartado 1 del artículo 95 de la Directiva (UE) 2015/2366, para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan.

Destinatarios

7. Estas Directrices se dirigen a los PSP, tal como se definen en el apartado 11 del artículo 4 de la Directiva (EU) 2015/2366 y se contemplan en la definición de «entidades financieras» del artículo 4, apartado 1, del Reglamento (UE) 1093/2010, y a las autoridades competentes, como se definen en el inciso i) del apartado 2 del artículo 4 de dicho Reglamento mediante referencia a la Directiva derogada 2007/64/CE[3] (actualmente, Directiva (UE) 2015/2366[4]).

Definiciones

8. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva (UE) 2015/2366 tienen idéntico significado en estas Directrices. Además, a los efectos de estas Directrices, se aplican las siguientes definiciones:

[2] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE, 2013/36/CE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35).

[3] Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, DO L 319 de 5.12.2007, p.1).

[4] Conforme al segundo párrafo del artículo 114 de la Directiva (UE) 2015/2366, las referencias a la Directiva derogada 2007/64/CE se entenderán hechas a la Directiva (UE) 2015/2366 y se leerán con arreglo a la tabla de correspondencias que figura en el anexo II de la Directiva (UE) 2015/2366.

Órgano de dirección	– Para los PSP que son entidades de crédito, este término tiene el mismo significado que en la definición del artículo 3, apartado 1, punto 7, de la Directiva 2013/36/UE.[5] – Para los PSP que son entidades de pago o entidades de dinero electrónico, este término significa los administradores o las personas responsables de la gestión del PSP y, en su caso, las personas responsables de la gestión de las actividades de servicios de pago del PSP. – 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 el proveedor de servicios de pago que tengan o puedan tener un impacto negativo en la integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad de los servicios relacionados con el pago.
Alta dirección	(a) Para los PSP que son entidades de crédito, este término tiene el mismo significado que en la definición del artículo 3, apartado 1, punto 9, de la Directiva 2013/36/UE. (b) Para los PSP que son entidades de pago y 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 del PSP y deben rendir cuentas de dicha gestión ante el órgano de dirección. (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.
Riesgo de seguridad	Riesgo resultante de la inadecuación o fallo de procesos internos o de sucesos externos que tengan o pudieran tener un impacto negativo en la disponibilidad, integridad o confidencialidad de los sistemas de información y comunicación (TIC) y/o de la información utilizada para la prestación de servicios de pago. Este riesgo incluye el riesgo de ciberataques o el riesgo derivado de una seguridad física inadecuada.
Apetito de riesgo	Nivel agregado y tipos de riesgo que una entidad está dispuesta a asumir dentro de su capacidad de riesgo, en línea con su modelo de negocio, a fin de lograr sus objetivos estratégicos.

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

3. Aplicación

Fecha de aplicación

9. Estas Directrices serán de aplicación a partir del 13 de enero de 2018.

4. Directrices

Directriz 1: Principio general

1.1 Todos los PSP deben cumplir la totalidad de las disposiciones establecidas en estas Directrices. El nivel de detalle debe ser proporcional al tamaño del PSP, así como a la naturaleza, al alcance, a la complejidad y al riesgo de los servicios concretos que el PSP presta o se propone prestar.

Directriz 2: Gobernanza

Marco de gestión de riesgos operativos y de seguridad

2.1 Los PSP establecerán un marco eficaz de gestión de riesgos operativos y de seguridad (en lo sucesivo, «marco de gestión de riesgos») que debe ser aprobado y revisado, al menos una vez al año, por el órgano de dirección y, en su caso, por la alta dirección. Dicho marco debe centrarse en las medidas de seguridad destinadas a mitigar los riesgos operativos y de seguridad y debe estar completamente integrado en los procesos generales de gestión de riesgos del PSP.

2.2 El marco de gestión de riesgos debe:

a) Incluir un documento exhaustivo relativo a la política de seguridad conforme a lo dispuesto en el artículo 5, apartado 1, letra j), de la Directiva (UE) 2015/2366.

b) Ser coherente con el apetito de riesgo del PSP.

c) Definir y asignar funciones y responsabilidades principales, así como los canales de comunicación pertinentes que sean necesarios para hacer cumplir las medidas de seguridad y para gestionar los riesgos operativos y de seguridad.

d) Establecer los procedimientos y sistemas, así como los mecanismos de continuidad del negocio, que sean necesarios para identificar, medir, controlar y gestionar la diversidad de riesgos que se derivan de las actividades del PSP relacionadas con el pago y a los cuales está expuesto.

2.3 Los PSP se asegurarán de que el marco de gestión de riesgos esté debidamente documentado y actualizado con las «lecciones aprendidas» durante su implementación y control, que estarán adecuadamente documentadas.

2.4 Los PSP se asegurarán de evaluar sin demora injustificada, antes de cualquier cambio importante en la infraestructura, los procesos o los procedimientos y después de cada incidente operativo o de seguridad grave que afecte a la seguridad de los servicios de pago que prestan, si es necesario realizar cambios o mejoras en el marco de gestión de riesgos.

Modelos de gestión y control de riesgos

2.5 Los PSP establecerán tres líneas de defensa eficaces, o un modelo interno de gestión y control de riesgos equivalente, para identificar y gestionar los riesgos operativos y de seguridad. Los PSP se asegurarán de que el modelo interno de control anteriormente mencionado tenga suficiente autoridad, independencia, recursos y canales de comunicación directa con el órgano de dirección y, según el caso, con la alta dirección.

2.6 Las medidas de seguridad establecidas en estas Directrices deberán ser auditadas por auditores con experiencia en seguridad informática y en servicios de pago, que sean operativamente independientes del PSP. La frecuencia y el foco de dichas auditorías deben tener en cuenta los correspondientes riesgos de seguridad.

Externalización

2.7 Los PSP garantizarán la eficacia de las medidas de seguridad establecidas en estas Directrices cuando las funciones operativas de los servicios de pago, incluidos los sistemas informáticos, estén externalizadas.

2.8 Los PSP se asegurarán de que los contratos y los acuerdos de nivel de servicio con los proveedores a los que hayan externalizado dichas funciones establezcan objetivos de seguridad, medidas y objetivos de rendimiento proporcionados y adecuados. Los PSP 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.

Directriz 3: Evaluación de riesgos

Identificación de funciones, procesos y activos

3.1 Los PSP identificarán, establecerán y actualizarán periódicamente un inventario de sus funciones de negocio, roles principales y procesos de apoyo con el fin de establecer la correspondencia entre la importancia de cada función, rol y proceso de apoyo, así como sus interdependencias en cuanto a los riesgos operativos y de seguridad.

3.2 Los PSP identificarán, establecerán y actualizarán periódicamente un inventario de los activos de información, tales como los sistemas TIC, sus configuraciones, otras infraestructuras y también las interconexiones con otros sistemas internos y externos, con el fin de poder gestionar los activos que apoyan sus funciones de negocio y procesos críticos.

Clasificación de funciones, procesos y activos

3.3 Los PSP clasificarán las funciones de negocio, los procesos de apoyo y los activos de información identificados en términos de criticidad.

Evaluación de riesgos de funciones, procesos y activos

3.4 Los PSP se asegurarán de que realizan una monitorización continua de las amenazas y vulnerabilidades y de que revisan periódicamente los escenarios de riesgo que afectan a sus funciones de negocio, procesos críticos y activos de información. Como parte de la obligación de realizar y presentar ante las autoridades competentes una evaluación actualizada y completa de los riesgos operativos y de seguridad asociados a los servicios de pago que prestan, así como de la adecuación de las medidas de mitigación y los mecanismos de control aplicados en respuesta a tales riesgos, tal como se estipula en el apartado 2 del artículo 95 de la Directiva (UE) 2015/2366, los PSP llevarán a cabo y documentarán una evaluación de riesgos, al menos anualmente o a intervalos más breves, según determine la autoridad competente, de las funciones, procesos y activos de información que hayan identificado y clasificado, con el fin de identificar y evaluar los principales riesgos operativos y de seguridad. Dicha evaluación de riesgos también se llevará a cabo antes de realizar cualquier cambio importante en la infraestructura, los procesos o los procedimientos que afecte a la seguridad de los servicios de pago.

3.5 Sobre la base de la evaluación de riesgos, los PSP determinarán si es necesario cambiar, y hasta qué punto, las medidas de seguridad existentes, las tecnologías utilizadas y los procedimientos o servicios de pago ofrecidos. Los PSP tendrán en cuenta el tiempo necesario para ejecutar estos cambios y el tiempo para adoptar medidas de seguridad transitorias adecuadas para minimizar los incidentes operativos o de seguridad, el fraude y los efectos potencialmente negativos en la prestación de servicios de pago.

Directriz 4: Protección

4.1 Los PSP establecerán y aplicarán medidas de seguridad preventivas contra los riesgos operativos y de seguridad identificados. Dichas medidas garantizarán un nivel de seguridad adecuado con arreglo a los riesgos identificados.

4.2 Los PSP establecerán y aplicarán un enfoque de «defensa en profundidad» mediante el establecimiento de controles en distintas capas que se aplican a las personas, los procesos y la tecnología, en los que cada capa sirva como red de seguridad a las capas anteriores. Se entiende que la defensa en profundidad define más de un control que se aplica al mismo riesgo, como el denominado principio de los cuatro ojos, la autenticación de doble factor, la segmentación de la red y varios cortafuegos.

4.3 Los PSP garantizarán la confidencialidad, la integridad y la disponibilidad de sus activos lógicos y físicos críticos y de sus recursos, así como de los datos de pago sensibles de sus usuarios de servicios de pago, tanto si están en reposo como si están en tránsito o en uso. Si los datos incluyen

información de carácter personal, dichas medidas se deben aplicar conforme al Reglamento (UE) 2016/679[6] o, en su caso, al Reglamento (CE) 45/2001.[7]

4.4 De manera continua, los PSP determinarán si los cambios en el entorno operativo existente influyen en las medidas de seguridad actuales o si es necesaria la adopción de medidas adicionales para mitigar el riesgo planteado. Dichos cambios deben formar parte del proceso formal de gestión de cambios del PSP, que debe velar por que los cambios se planifiquen, se prueben, se documenten y se autoricen de forma adecuada. En función de las amenazas de seguridad observadas y de las modificaciones realizadas, se deberán realizar las pruebas oportunas para incorporar escenarios de posibles ataques relevantes y conocidos.

4.5 A la hora de diseñar, desarrollar y prestar servicios de pago, los PSP velarán por que se apliquen los principios de segregación de funciones y de mínimo privilegio. Los PSP prestarán especial atención a la separación de los entornos informáticos, en particular, de los entornos de desarrollo, pruebas y producción.

Integridad y confidencialidad de datos y sistemas

4.6 A la hora de diseñar, desarrollar y prestar servicios de pago, los PSP se asegurarán de que la recopilación, encaminamiento, tratamiento, almacenamiento o archivado y visualización de los datos de pago sensibles del usuario de servicios de pago sean adecuados, oportunos y se limiten a lo necesario para la prestación de sus servicios de pago.

4.7 Los PSP comprobarán de manera periódica que el software utilizado para la prestación de los servicios de pago, incluido el software de pago de los usuarios, está actualizado y que se han instalado los parches de seguridad críticos. Los PSP se asegurarán de que cuentan con mecanismos de comprobación de la integridad con el fin de verificar la integridad del software, del firmware y de la información de sus servicios de pago.

Seguridad física

4.8 Los PSP deben disponer de medidas de seguridad física adecuadas, en particular, para proteger los datos de pago sensibles de los usuarios de servicios de pago, así como los sistemas TIC utilizados para prestar servicios de pago.

Control de acceso

4.9 El acceso físico y lógico a los sistemas TIC se permitirá únicamente a las personas autorizadas. La autorización se asignará conforme a las tareas y responsabilidades del personal y se limitará a

[6] Reglamento (UE) 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).

[7] Reglamento (CE) no 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

aquellas personas que cuentan con la formación y la supervisión adecuadas. Los PSP establecerán controles de forma que dicho acceso a los sistemas TIC quede restringido de manera fiable a quienes lo necesiten para el desempeño de sus funciones. El acceso electrónico mediante aplicaciones a los datos y sistemas se limitará al mínimo imprescindible para prestar el servicio correspondiente.

4.10 Los PSP establecerán controles fuertes sobre los accesos privilegiados al sistema mediante la estricta limitación y la estrecha supervisión del personal con amplios permisos de acceso al sistema. Se implantarán controles como accesos basados en roles, registro y revisión de las actividades de los usuarios privilegiados, autenticación fuerte y seguimiento de anomalías. Los PSP gestionarán los derechos de acceso a los activos de información y a sus procesos de apoyo según el principio de «necesidad de conocer». Los derechos de acceso se revisarán de manera periódica.

4.11 Los registros de acceso 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 las Directrices 3.1 y 3.2, sin perjuicio de los requisitos de conservación estipulados en la legislación nacional y de la Unión Europea. Los PSP usarán dicha información para facilitar la identificación y la investigación de actividades anómalas que se hayan detectado en la prestación de los servicios de pago.

4.12 Con el fin de garantizar una comunicación segura y reducir el riesgo, el acceso de administración remota a componentes TIC críticos solo se concederá según el principio de «necesidad de conocer» y solo en caso de que se usen soluciones de autenticación fuerte.

4.13 El funcionamiento de los productos, herramientas y procedimientos relacionados con los procesos de control de acceso debe evitar que los procesos de control de acceso se puedan eludir o poner en peligro. Esto incluye el alta, la entrega, la revocación y la retirada de los correspondientes productos, herramientas y procedimientos.

Directriz 5: Detección

Monitorización continua y detección

5.1 Los PSP establecerán e implantarán procesos y capacidades para monitorizar de manera continua las funciones de negocio, los procesos de apoyo y los activos de información con el fin de detectar actividades anómalas en la prestación de servicios de pago. Como parte de esta monitorización continua, los PSP contarán con capacidades adecuadas y eficaces para detectar intrusiones físicas o lógicas, así como el quebrantamiento de la confidencialidad, la integridad y la disponibilidad de los activos de información utilizados en la prestación de los servicios de pago.

5.2 Los procesos de monitorización continua y detección deben cubrir lo siguiente:

a) Los factores internos y externos relevantes, incluidas las funciones administrativas de negocio y TIC.

b) Las operaciones, con el fin de detectar el uso indebido del acceso por parte de los proveedores de servicios o de otras entidades, y

c) Las amenazas potenciales internas y externas.

5.3 Los PSP implantarán medidas de detección para identificar posibles filtraciones de información, códigos maliciosos y otras amenazas de seguridad, y vulnerabilidades de dominio público del software y el hardware. Asimismo, comprobarán las nuevas actualizaciones de seguridad que correspondan.

Monitorización y comunicación de incidentes operativos o de seguridad

5.4 Los PSP determinarán los criterios de seguridad y los umbrales adecuados para clasificar un evento como incidente operativo 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 aviso para permitir que el PSP realice una detección temprana de los incidentes operativos o de seguridad.

5.5 Los PSP establecerán las estructuras organizativas y los procesos adecuados para asegurar que la monitorización, la gestión y el seguimiento de los incidentes operativos o de seguridad se realizan de manera consistente e integrada.

5.6 Los PSP establecerán un procedimiento para comunicar a la alta dirección dichos incidentes operativos o de seguridad, así como las reclamaciones de los clientes relacionadas con la seguridad.

Directriz 6: Continuidad del negocio

6.1 Los PSP establecerán una sólida gestión de la continuidad del negocio, con el fin de maximizar su capacidad para prestar servicios de pago de forma continuada y limitar las pérdidas en caso de interrupciones graves de la actividad.

6.2 Para establecer una sólida gestión de la continuidad del negocio, los PSP analizarán con detenimiento su exposición a interrupciones graves de la actividad y evaluarán cuantitativa y cualitativamente su posible impacto, sirviéndose de datos internos o externos y de análisis de escenarios. Según las funciones críticas, los procesos, los sistemas, las operaciones y las interdependencias que se hayan identificado y clasificado conforme a las Directrices 3.1 a 3.3, los PSP priorizarán las acciones de continuidad de negocio mediante un enfoque basado en riesgo, el cual se puede basar en la evaluación de riesgos llevada a cabo según la Directriz 3. Dependiendo del modelo de negocio del PSP, esto podría, por ejemplo, facilitar el procesamiento adicional de las operaciones críticas mientras continúan las medidas de reparación.

6.3 Según el análisis llevado a cabo conforme a la Directriz 6.2, los PSP establecerán:

a) Planes de continuidad de negocio para garantizar que puede reaccionar de manera adecuada a las emergencias y que es capaz de mantener sus actividades críticas, y

b) Medidas de mitigación que se adoptarán en caso de cese de la prestación de sus servicios de pago y de la extinción de los contratos existentes con el fin de evitar efectos adversos sobre los sistemas de pago y sobre los usuarios de servicios de pago y de asegurar la ejecución de las operaciones de pago pendientes.

Planificación de la continuidad del negocio basada en escenarios

6.4 Los PSP considerarán varios escenarios distintos a los que podrían estar expuestos, incluidos escenarios extremos pero plausibles, y evaluarán su posible impacto.

6.5 Basándose en el análisis llevado a cabo con arreglo a la Directriz 6.2 y los escenarios plausibles identificados según la Directriz 6.4, el PSP desarrollará planes de respuesta y recuperación que deberán tener las siguientes características:

a) Estar centrados en el impacto sobre el funcionamiento de las funciones críticas, los procesos, los sistemas, las operaciones y sus interdependencias.

b) Estar documentados y a disposición de las unidades de negocio y de apoyo y ser fácilmente accesibles en caso de emergencia, y

c) Estar actualizados teniendo en cuenta las lecciones aprendidas durante las pruebas, los nuevos riesgos identificados, las amenazas y los cambios en los objetivos y prioridades de recuperación.

Prueba de los planes de continuidad de negocio

6.6 Los PSP probarán sus planes de continuidad de negocio y se asegurarán de que el funcionamiento de sus funciones críticas, procesos, sistemas, operaciones e interdependencias se prueban al menos una vez al año. Los planes servirán de apoyo a los objetivos de protección y, si fuera necesario, de restablecimiento de la integridad y disponibilidad de sus operaciones y de la confidencialidad de sus activos de información.

6.7 Los planes se actualizarán al menos una vez al año, en función de los resultados de las pruebas, la información sobre las amenazas actuales, el intercambio de información y las lecciones aprendidas de eventos anteriores y de los cambios en los objetivos de recuperación, así como del análisis de escenarios plausibles desde el punto de vista operativo y técnico que aún no se hayan materializado y, si resulta oportuno, después de cualquier cambio en los sistemas y en los procesos. Los PSP consultarán a las partes implicadas pertinentes, tanto internas como externas, y se coordinarán con ellas durante el establecimiento de sus planes de continuidad de negocio.

6.8 Las pruebas de los planes de continuidad de negocio de los PSP:

a) Incluirán un conjunto adecuado de escenarios, tal como se indica en la Directriz 6.4.

b) Estarán diseñadas para poner en cuestión los supuestos en los que se basan los planes de continuidad de negocio, incluidos los planes de comunicación de crisis y los procedimientos de gobierno interno.

c) Incluirán procedimientos para verificar la capacidad de su personal y de sus procesos para responder de manera adecuada a los escenarios anteriormente mencionados.

6.9 Los PSP realizarán un seguimiento periódico de la eficacia de sus planes de continuidad de negocio y documentarán y analizarán cualquier problema o fallo que se derive de las pruebas.

Comunicación de crisis

6.10 En el caso de que ocurra una interrupción o una emergencia, y durante la implantación de los planes de continuidad de negocio, los PSP se asegurarán de que disponen de medidas eficaces de comunicación de crisis que permitan que todas las partes implicadas, incluidos los proveedores de servicios externos, sean informados de manera oportuna y adecuada.

Directriz 7: Prueba de las medidas de seguridad

7.1 Los PSP establecerán e implementarán un marco de pruebas que valide la robustez y eficacia de las medidas de seguridad y se asegurarán de que el marco de pruebas se adapte para considerar las nuevas amenazas y vulnerabilidades identificadas a través de las actividades de control de riesgos.

7.2 Los PSP se asegurarán de que se realicen pruebas en caso de que se produzcan cambios en la infraestructura, los procesos o los procedimientos y de que se realicen cambios como consecuencia de incidentes operativos o de seguridad graves.

7.3 El marco de pruebas también abarcará las medidas de seguridad correspondientes a i) los terminales y dispositivos de pago usados para la prestación de servicios de pago, ii) los terminales y dispositivos de pago usados para la autenticación del usuario de servicios de pago y iii) los dispositivos y el software proporcionados por el PSP al usuario de servicios de pago para generar o recibir un código de autenticación.

7.4 El marco de pruebas garantizará que las pruebas:

a) Se realizan como parte del procedimiento formal de gestión del cambio del PSP para asegurar su robustez y eficacia.

b) Se llevan a cabo por parte de técnicos de pruebas independientes que tienen suficientes conocimientos, capacidades y experiencia en la prueba de medidas de seguridad de servicios de pago y no participan en el desarrollo de las medidas de seguridad de los correspondientes servicios o sistemas de pago que se vayan a probar, al menos, en el caso de las pruebas finales antes de poner en marcha las medidas de seguridad, y

c) Incluyen exploraciones sistemáticas de vulnerabilidades y pruebas de penetración adecuadas al nivel de riesgo identificado de los servicios de pago.

7.5 Los PSP realizarán pruebas continuas y repetidas de las medidas de seguridad de sus servicios de pago. En el caso de los sistemas que son críticos para la prestación de sus servicios de pago (tal como se describe en la Directriz 3.2), dichas pruebas se llevarán a cabo al menos una vez al año.

Los sistemas no críticos se probarán de manera periódica según un enfoque basado en riesgo, pero, como mínimo, cada tres años.

7.6 Los PSP monitorizarán y evaluarán los resultados de las pruebas realizadas y actualizarán sus medidas de seguridad en consecuencia y sin demoras injustificadas en el caso de los sistemas críticos.

Directriz 8: Conocimiento de la situación y aprendizaje continuo

Panorama de amenazas y conocimiento de la situación

8.1 Los PSP establecerán e implantarán procesos y estructuras organizativas para identificar y monitorizar de forma constante las amenazas operativas y de seguridad que podrían afectar de manera importante a su capacidad para prestar los servicios de pago.

8.2 Los PSP analizarán los incidentes operativos o de seguridad que se hayan identificado o que hayan ocurrido dentro o fuera de la entidad. Los PSP tendrán en cuenta las principales lecciones aprendidas de dichos análisis y actualizarán las medidas de seguridad en consecuencia.

8.3 Los PSP realizarán un seguimiento activo de los desarrollos tecnológicos para asegurar que son conscientes de los riesgos de seguridad.

Programas de formación y de concienciación en seguridad

8.4 Los PSP establecerán un programa de formación para todo el personal para asegurarse de que cuenta con los conocimientos necesarios para desempeñar sus tareas y responsabilidades conforme a las políticas y procedimientos de seguridad pertinentes, con el fin de reducir errores humanos, robos, fraudes, usos indebidos o pérdidas. Los PSP se asegurarán de que el programa de formación prevea la formación del personal al menos una vez al año, y con mayor frecuencia si es necesario.

8.5 Los PSP se asegurarán de que el personal que desempeñe roles principales identificados con arreglo a la Directriz 3.1 reciban formación específica sobre seguridad de la información una vez al año, o con mayor frecuencia si es necesario.

8.6 Los PSP establecerán e implantarán programas periódicos de concienciación en seguridad con el fin de formar a su personal y de tratar los riesgos relacionados con la seguridad de la información. Estos programas exigirán que el personal del PSP informe de cualquier actividad inusual o incidente.

Directriz 9: Gestión de la relación con los usuarios de servicios de pago

Concienciación de los usuarios de servicios de pago sobre los riesgos de seguridad y las acciones de reducción del riesgo

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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.