EBA/GL/2014/12_Rev1

19 de diciembre de 2014

Directrices definitivas

sobre la seguridad de los pagos por internet

Índice

Directrices sobre la seguridad de los pagos por internet

Rango jurídico de las presentes Directrices

El presente documento contiene directrices emitidas en virtud del artículo 16 del 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 2009/78/CE de la Comisión («Reglamento de la ABE»). Con arreglo al artículo 16, apartado 3, del Reglamento de la ABE, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

Las directrices exponen el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera y sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. En consecuencia, la ABE espera que todas las autoridades competentes y entidades financieras a las que se dirigen las directrices las cumplan. Las autoridades competentes a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de supervisión de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que determinadas directrices vayan dirigidas principalmente a las entidades.

Requisitos de notificación

De conformidad con el artículo 16, apartado 3, del Reglamento de la ABE, las autoridades competentes deberán notificar a la ABE, a más tardar el 5 de mayo de 2015, si cumplen o se proponen cumplir estas directrices o, en caso negativo, los motivos del incumplimiento. A falta de notificación en ese plazo, la ABE considerará que las autoridades competentes no la cumplen. Las notificaciones se presentarán remitiendo el modelo incluido en la sección 5 a compliance@eba.europa.eu, con la referencia «EBA/GL/2014/12». Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes.

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

Título I. Ámbito de aplicación y definiciones

Ámbito de aplicación

1. Las presentes Directrices establecen un conjunto de requisitos mínimos relativos a la seguridad de los pagos por internet. Las Directrices se basan en las normas de la Directiva 2007/64/CE[1] («Directiva sobre servicios de pago», DSP) relativa a los requisitos de información aplicables a los servicios de pago y las obligaciones de los proveedores de servicios de pago (PSP) en relación con la prestación de dichos servicios. Además, el artículo 10, apartado 4, de la Directiva exige que las entidades de pago dispongan de sólidos procedimientos de gobierno corporativo y mecanismos adecuados de control interno.

2. Las presentes Directrices se aplican a la prestación de los servicios de pago ofrecidos a través de internet por los PSP tal como se definen en el artículo 1 de la Directiva.

3. Las presentes Directrices se dirigen a las entidades financieras definidas en el artículo 4, apartado 1, del Reglamento (UE) nº 1093/2010 y a las autoridades competentes definidas en el artículo 4, apartado 2, de dicho Reglamento. Las autoridades competentes de los 28 Estados miembros de la Unión Europea deberían garantizar la aplicación de las presentes Directrices por parte de los PSP, tal como se definen en el artículo 1 de la DSP, bajo su supervisión.

4. Además, las autoridades competentes podrán solicitar a los PSP que informen a la autoridad competente de su cumplimento con las presentes Directrices.

5. Las presentes Directrices no afectan a la validez de las «Recomendaciones para la seguridad de los pagos por internet» del Banco Central Europeo (el «Informe»)[2]. En concreto, el Informe sigue representando el documento respecto al que los bancos centrales, en el ejercicio de su función de vigilancia de los sistemas e instrumentos de pago, deberán evaluar el cumplimiento en materia de seguridad de los pagos por internet.

6. Las presentes Directrices constituyen unas expectativas mínimas, sin perjuicio de la responsabilidad de los PSP de tener que efectuar un seguimiento y evaluación de los riesgos asociados a sus operaciones de pago, desarrollar sus propias políticas de seguridad específicas y aplicar medidas de seguridad, contingencia, gestión de incidentes y continuidad de negocio adecuadas y proporcionales a los riesgos inherentes a los servicios de pago prestados.

[1] 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, 5.12.2007,

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

7. El propósito de las presentes Directrices es definir los requisitos mínimos comunes para los servicios de pago por internet enumerados a continuación, independientemente del dispositivo de acceso utilizado:

    - [tarjetas] la realización de operaciones de pago con tarjeta, incluidas las tarjetas virtuales, a través de internet, así como el registro de los datos relativos a la tarjeta de pago para su empleo en «soluciones tipo monedero»;

    - [transferencias] la realización de transferencias a través de internet;

    - [mandato electrónico] la emisión y modificación de mandatos electrónicos relativos a adeudos domiciliados;

    - [dinero electrónico] transferencias de saldos entre dos cuentas de dinero electrónico a través de internet.

8. Cuando las presentes Directrices indiquen solamente un resultado, este podrá alcanzarse a través de distintos medios. Aparte de los requisitos establecidos en las presentes Directrices, estas también proporcionan ejemplos de buenas prácticas (en el anexo 1) que se recomienda a los PSP seguir, si bien no se les obliga a ello.

9. Cuando la prestación de servicios e instrumentos de pago se ofrezca a través de un régimen de pago (por ejemplo, regímenes de pago con tarjeta, de transferencias, de adeudos domiciliados, etc.), las autoridades competentes y el banco central pertinente deberían colaborar en el ejercicio de su función de vigilancia sobre los instrumentos de pago, para garantizar una aplicación consistente de las Directrices por parte de los agentes responsables del funcionamiento del régimen.

10. Los integradores de pagos[3] que ofrecen servicios de iniciación de pagos se consideran bien adquirentes de servicios de pago por internet (y, por tanto, PSP), bien proveedores externos de servicios técnicos para los regímenes pertinentes o para los PSP. En el último caso, se deberá exigir contractualmente a los integradores de pagos que cumplan con las presentes Directrices.

11. Quedan excluidos del ámbito de aplicación de las Directrices:

    - otros servicios de internet prestados por un PSP a través de su sitio web para la realización de pagos (por ejemplo, corretaje electrónico, contratos en línea);

    - los pagos en los que la orden se da por correo, teléfono, mensaje de voz o utilizando tecnología basada en SMS;

[3] Los integradores de pago proporcionan al beneficiario (es decir, al comercio electrónico) una interfaz estandarizada para los servicios de iniciación de pagos prestados por los PSP.

- los pagos por móvil distintos en los que el dispositivo móvil no se emplee exclusivamente como un navegador de internet;

- las transferencias realizadas a través de un tercero al que el cliente facilita el acceso a su cuenta de pago;

- las operaciones de pago realizadas por una empresa a través de redes dedicadas;

- los pagos con tarjetas de prepago, virtuales o físicas, no recargables y anónimas cuando no existe ninguna relación continuada entre el emisor y el titular de la tarjeta;

- la compensación y liquidación de las operaciones de pago.

Definiciones

12. A efectos de las presentes Directrices, y además de las definiciones proporcionadas en la DSP, se aplican las siguientes definiciones:

- Por *autenticación* se entiende un procedimiento que permita al PSP comprobar la identidad del cliente;

- Por *autenticación fuerte del cliente* se entiende, a efectos de estas Directrices, un procedimiento basado en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión e inherencia: i) algo que solo conoce el usuario, por ejemplo, una contraseña, código o número de identificación personal fijos; ii) algo que solo posee el usuario, por ejemplo, *token*, tarjeta inteligente, teléfono móvil; iii) algo que caracteriza al propio usuario, por ejemplo, una característica biométrica, como su huella dactilar. Además, los elementos seleccionados deben ser independientes entre sí; es decir, la violación de uno no debe comprometer la seguridad de los otros. Al menos uno de los elementos no debe ser reutilizable ni reproducible (salvo para la inherencia) y su sustracción, de manera subrepticia, a través de internet no debe resultar posible. El procedimiento de autenticación fuerte se debe diseñar de tal forma que proteja la confidencialidad de los datos de autenticación.

- Por *autorización* se entiende un procedimiento para comprobar si el cliente o PSP tiene el derecho a realizar una determinada acción, por ejemplo, el derecho a transferir fondos o tener acceso a datos sensibles.

- Por *credenciales* se entiende la información, generalmente confidencial, proporcionada por el cliente o PSP a efectos de la autenticación. Las credenciales también pueden significar la posesión de una herramienta física que contenga la información (por ejemplo, generador de contraseña de un solo uso, tarjeta inteligente), o algo que el usuario memorice o represente (como una característica biométrica).

- Por *incidente de seguridad grave en los pagos* se entiende un incidente que tenga o pueda tener un impacto material sobre la seguridad, integridad o continuidad de los sistemas del PSP que soporten la operativa de pago y/o sobre la seguridad de los datos de pago sensibles o sobre los fondos. La evaluación de la importancia debería tener en cuenta el número de clientes potencialmente afectados, el importe en riesgo y el impacto sobre otros PSP o infraestructuras de pago.

- Por *análisis de riesgo de las operaciones* se entiende la evaluación del riesgo relacionada con una operación específica teniendo en cuenta criterios como, por ejemplo, los patrones de pago del cliente (comportamiento), el valor de la operación correspondiente, el tipo de producto y el perfil del beneficiario.

- Por *tarjetas virtuales* se entiende una solución de pago con tarjeta, que se puede usar para comprar en internet, en la que se genera un número de tarjeta, temporal y alternativo, con un periodo de validez reducido, un uso limitado y una cuantía de gasto máxima predefinida.

- Por *soluciones tipo monedero* se entienden aquellas soluciones que permiten al cliente registrar los datos relacionados con uno o más instrumentos de pago para realizar pagos con varios comercios electrónicos.

Título II. Directrices sobre la seguridad de los pagos por internet

Entorno general de control y seguridad

Gobernanza

1. Los PSP aplicarán y revisarán periódicamente una política de seguridad formal para los servicios de pago por internet.

   1.1 La política de seguridad se documentará adecuadamente y se revisará periódicamente (en línea con la Directriz 2.4) y ser aprobada por la alta dirección. Dicha política definirá los objetivos de seguridad y la propensión al riesgo.

   1.2 La política de seguridad definirá funciones y responsabilidades, incluida una función de gestión de riesgos que informe directamente al órgano de administración, así como los canales de comunicación para los servicios de pago que se presten por internet, incluyendo la gestión de los datos de pago sensibles respecto a la evaluación, control y mitigación de riesgos.

Evaluación de riesgos

2. Los PSP realizarán y documentarán, de manera exhaustiva, ejercicios de evaluación de riesgos relativos a la seguridad de los pagos por internet y servicios relacionados, tanto con anterioridad al establecimiento del servicio o servicios como de forma periódica, una vez establecidos.

   2.1 Los PSP, a través de su función de gestión de riesgos, realizarán y documentarán ejercicios de evaluación de riesgos detallados relativos a los pagos por internet y servicios relacionados. Los PSP considerarán los resultados del seguimiento continuo de las amenazas a la seguridad relacionadas con los servicios de pago por internet que ofrecen o tienen previsto ofrecer, teniendo en cuenta: i) las soluciones tecnológicas empleadas, ii) los servicios externalizados a proveedores externos, y iii) el entorno técnico de los clientes. Los PSP considerarán los riesgos asociados a las plataformas tecnológicas escogidas, la arquitectura de las aplicaciones, las técnicas y rutinas de programación tanto suyas[4] como de sus clientes[5], así como los resultados del proceso de seguimiento de incidentes de seguridad (véase la Directriz 3).

   2.2 Sobre esa base, los PSP determinarán hasta qué punto son necesarios cambios en las medidas de seguridad existentes, en las tecnologías utilizadas y en los procedimientos o servicios ofrecidos. Los PSP tendrán en cuenta el tiempo necesario para ejecutar

[4] Por ejemplo, la susceptibilidad del sistema a la piratería de las sesiones de pago, inyección de código SQL, scripts de sitios, desbordamientos del buffer, etc.

[5] Por ejemplo, los riesgos asociados al uso de aplicaciones multimedia, complementos (plug-ins) del navegador, marcos, enlaces externos, etc.

estos cambios (incluida su implementación por parte del cliente) y tomarán las medidas transitorias adecuadas para minimizar los incidentes de seguridad y el fraude, así como los efectos potencialmente negativos.

2.3 El ejercicio de evaluación de riesgos abordará la necesidad de proteger y salvaguardar los datos de pago sensibles.

2.4 Los PSP realizarán una revisión de los escenarios de riesgo y de las medidas de seguridad existentes después de producirse un incidente grave que afecte a sus servicios, antes de efectuar una modificación importante en la infraestructura o los procedimientos y cuando se identifiquen nuevas amenazas a través de las actividades de seguimiento de los riesgos. Además, con una periodicidad mínima anual, se efectuará una revisión general del ejercicio de evaluación de riesgos. Los resultados de las evaluaciones de riesgos y sus revisiones se enviarán a la alta dirección para su aprobación.

Control y notificación de incidentes

3. Los PSP garantizarán un control, gestión y seguimiento consistente e integrado de los incidentes de seguridad, incluidas las quejas de los clientes relacionadas con la seguridad. Los PSP establecerán un procedimiento para notificar tales incidentes a la administración y, en el caso de incidentes de seguridad graves en los pagos, a las autoridades competentes.

3.1 Los PSP dispondrán de un proceso para controlar, gestionar y realizar un seguimiento de los incidentes de seguridad y las reclamaciones de los clientes relacionadas con la seguridad e informar de tales incidentes a la administración.

3.2 Los PSP contarán con un procedimiento para notificar, de forma inmediata, a las autoridades competentes (es decir, a las autoridades de supervisión y de protección de datos), cuando estas existan, los incidentes de seguridad graves que afecten a los servicios de pago prestados.

3.3 Los PSP contarán con un procedimiento que les permita cooperar con las fuerzas y cuerpos de seguridad pertinentes en caso de incidentes graves que afecten a la seguridad de los pagos, incluidas las violaciones de datos.

3.4 Los PSP adquirentes impondrán contractualmente a los comercios electrónicos con los que contraten y que almacenen, procesen o transmitan datos de pago sensibles cooperar en relación a los incidentes graves que afecten a la seguridad en los pagos, incluidas las violaciones de datos, tanto con ellos mismos como con las fuerzas y cuerpos de seguridad. Cuando llegue a conocimiento de un PSP que un comercio electrónico no coopera según lo establecido en el contrato, dicho PSP tomará medidas para exigir el cumplimiento de esta obligación contractual o para resolver el contrato.

Control y mitigación de riesgos

4. Los PSP adoptarán medidas de seguridad en consonancia con sus políticas de seguridad con el fin de mitigar los riesgos identificados. Dichas medidas incorporarán varios niveles de defensa de la seguridad, de modo que el fracaso de una línea de defensa se vea mitigado por la siguiente («*defense in depth*»).

4.1 A la hora de diseñar, desarrollar y mantener servicios de pago por internet, los PSP prestarán especial atención a mantener una adecuada segregación de las responsabilidades en los entornos de las tecnologías de la información (TI) (por ejemplo, los entornos de desarrollo, pruebas y producción), y la aplicación adecuada del «principio del privilegio mínimo» como base para una gestión sólida de identidades y accesos[6].

4.2 Los PSP dispondrán de soluciones de seguridad adecuadas para proteger las redes, los sitios web, los servidores y los enlaces de comunicación frente a abusos o ataques. Los PSP liberarán los servidores de toda función superflua para protegerlos (fortalecerlos) y eliminar o reducir la vulnerabilidad de las aplicaciones en riesgo. El acceso de las distintas aplicaciones a los datos y recursos necesarios se limitará a lo mínimo de conformidad con el «principio del privilegio mínimo». Para restringir el uso de sitios web «falsos» (que imitan a los sitios auténticos de los PSP), los sitios web transaccionales que ofrecen servicios de pago por internet se identificarán mediante certificados de validación expedidos en nombre del PSP o mediante otros métodos de autenticación similares.

4.3 Los PSP contarán con procesos adecuados para monitorizar, realizar seguimientos y restringir el acceso a: i) datos de pago sensibles y ii) recursos lógicos y físicos críticos, tales como redes, sistemas, bases de datos, módulos de seguridad, etc. Los PSP crearán, almacenarán y analizarán registros y pistas de auditoría adecuados.

4.4 A la hora de diseñar[7], desarrollar y mantener los servicios de pago por internet, los PSP garantizarán que la minimización de datos[8] sea un componente básico de la funcionalidad principal: la recopilación, enrutamiento, procesamiento, almacenamiento y/o archivado, y la visualización de datos de pago sensibles se limitarán a lo estrictamente necesario.

4.5 Las medidas de seguridad para los servicios de pago por internet se probarán bajo la supervisión de la función de gestión de riesgos para garantizar su solidez y efectividad. Cualquier modificación estará sujeta a un proceso formal de gestión de cambios que garantice que estos se planifiquen, prueben, documenten y autoricen de forma

[6] «Cada programa y cada usuario privilegiado del sistema deben operar usando el menor número de privilegios necesarios para completar el trabajo.» Véase Saltzer, J.H. (1974), «Protection and the Control of Information Sharing in Multics», Communications of the ACM, Vol. 17, Nº 7, p. 388.

[7] Privacidad desde el diseño.

[8] La minimización de datos hace referencia a la política de recopilación de la menor cantidad de información personal necesaria para realizar una determinada función.

adecuada. Sobre la base de las modificaciones realizadas y de las amenazas de seguridad observadas, las pruebas se repetirán periódicamente e incluirán escenarios de posibles ataques relevantes y conocidos.

4.6 Las medidas de seguridad de los PSP para los servicios de pago por internet se auditarán de forma periódica para garantizar su solidez y efectividad. La implementación y el funcionamiento de los servicios de pago por internet también serán objeto de auditoría. La frecuencia y el enfoque de tales auditorías tendrán en cuenta y serán proporcionales a los correspondientes riesgos de seguridad. Las auditorías serán realizadas por expertos de confianza e independientes (internos o externos). Estos expertos no deberán estar bajo ninguna circunstancia involucrados en el desarrollo, la implementación o la gestión operativa de los servicios de pago que se presten por internet.

4.7 Cuando los PSP externalicen funciones relacionadas con la seguridad de los servicios de pago por internet, el contrato incluirá disposiciones que exijan el cumplimento de los principios y orientaciones establecidas en las presentes Directrices.

4.8 Los PSP que ofrezcan servicios de adquisición exigirán contractualmente a los comercios electrónicos que manejen (es decir, almacenen, procesen o transmitan) datos de pago sensibles que apliquen medidas de seguridad en su infraestructura de TI, en consonancia con la Directrices 4.1 a 4.7, para evitar la sustracción de dichos datos de pago sensibles a través de sus sistemas. Cuando llegue a conocimiento de un PSP que un comercio electrónico no cuenta con las medidas de seguridad necesarias, emprenderá acciones para exigir el cumplimiento de esta obligación contractual o para resolver el contrato.

Trazabilidad

5. Los PSP contarán con procesos que garanticen que todas las operaciones, así como el flujo de proceso del mandato electrónico quedan adecuadamente registrados.

5.1 Los PSP garantizarán que su servicio incorpora los mecanismos de seguridad para el registro detallado de los datos de las operaciones y de los mandatos electrónicos, incluido el número secuencial de la operación, el fechado de los datos de la operación, las modificaciones en la determinación de parámetros así como el acceso a los datos de las operaciones y los mandatos electrónicos.

5.2 Los PSP implementarán archivos de registros que permitan el rastreo de cualquier incorporación, modificación o eliminación de datos de operaciones y mandatos electrónicos.

5.3 Los PSP solicitarán y analizarán los datos de las operaciones y mandatos electrónicos y garantizarán que cuentan con las herramientas necesarias para evaluar los archivos de

registro. Las correspondientes aplicaciones solo estarán disponibles para el personal autorizado.

Medidas específicas de control y seguridad para los pagos por internet

Identificación inicial de los clientes e información

6. Los clientes serán identificados de manera adecuada conforme a la legislación europea contra el blanqueo de capitales[9] y se confirmará su disposición para utilizar los servicios de pagos por internet con carácter previo al acceso a los mismos. Los PSP proporcionarán al cliente información «previa», «periódica» o «ad hoc», según proceda, sobre los requisitos necesarios (por ejemplo, equipos, procedimientos) para llevar a cabo operaciones de pago seguras por internet y sobre los riesgos inherentes.

6.1 Los PSP se asegurarán de que sus clientes se han sometido a los procedimientos de debida diligencia (*«due diligence»*) oportunos y que ha proporcionado los documentos de identificación adecuados[10] y la información pertinente antes de otorgarles el acceso a los servicios de pago por internet.[11]

6.2 Los PSP se asegurarán de que la información previa[12] proporcionada al cliente contiene detalles específicos relacionados con los servicios de pago por internet. Estos incluirán, según proceda:

- información clara sobre cualquier requisito relativo al equipo del cliente, software o cualquier otra herramienta necesaria (por ejemplo, software antivirus, cortafuegos);
- pautas para el uso adecuado y seguro de las credenciales de seguridad personalizadas;
- una descripción detallada del procedimiento que debe seguir el cliente para iniciar y autorizar una operación de pago y/u obtener información, incluidas las consecuencias de cada acción;

[9] Por ejemplo, la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo. DO L 309 de 25.11.2005, pp. 15-36. Véase también la Directiva 2006/70/CE de la Comisión, de 1 de agosto de 2006, por la que se establecen disposiciones de aplicación de la Directiva 2005/60/CE del Parlamento Europeo y del Consejo en lo relativo a la definición de «personas del medio político» y los criterios técnicos aplicables en los procedimientos simplificados de diligencia debida con respecto al cliente así como en lo que atañe a la exención por razones de actividad financiera ocasional o muy limitada. DO L 214 de 4.8.2006, pp. 29-34.

[10] Por ejemplo, pasaporte, documento nacional de identidad o firma electrónica avanzada.

[11] El proceso de identificación del cliente se realiza sin perjuicio de cualquier exención prevista en la legislación existente contra el blanqueo de capitales. Los PSP no necesitan llevar a cabo un proceso de identificación del cliente separado para los servicios de pago por internet, si dicha identificación ya se ha realizado, por ejemplo, para otros servicios existentes de pago o para la apertura de una cuenta.

[12] Esta información complementa al artículo 42 de la DSP que especifica la información que el PSP debe proporcionar al usuario de los servicios de pago antes de firmar un contrato para la prestación de servicios de pago.

- pautas para el uso adecuado y seguro de todo el hardware y software proporcionado al cliente;

- los procedimientos que se deberán seguir en caso de pérdida o robo de las credenciales de seguridad personalizadas o del hardware o software del cliente para iniciar una sesión o realizar operaciones;

- los procedimientos que se deberán seguir si se detecta o sospecha que se ha producido un abuso;

- una descripción de las responsabilidades y obligaciones del PSP y del cliente, respectivamente, en relación con el uso del servicio de pagos por internet.

6.3 Los PSP se asegurarán de que el contrato marco con el cliente especifica que el PSP podrá bloquear una operación concreta o el instrumento de pago[13] por motivos de seguridad. Establecerá el método y las condiciones de información al cliente y cómo puede ponerse en contacto el cliente con el PSP para «desbloquear» el servicio u operación de pago por internet, de acuerdo con la DSP.

[13] Véase el artículo 55 de la DSP sobre las limitaciones de la utilización del instrumento de pago.

Autenticación fuerte de los clientes

7. Tanto la iniciación de las operaciones de pago por internet como el acceso a datos de pago sensibles estarán protegidos mediante una autenticación fuerte del cliente. Los PSP contarán con un procedimiento de autenticación fuerte del cliente en línea con la definición proporcionada en estas Directrices.

   7.1 [transferencias/mandato electrónico/dinero electrónico] Los PSP realizarán una autenticación fuerte del cliente para autorizar sus operaciones de pago por internet (incluidas las transferencias que se agrupen en lotes) y la emisión o modificación de los mandatos electrónicos relativos a adeudos domiciliados. Sin embargo, los PSP podrán considerar la adopción de medidas alternativas para la autenticación del cliente en los siguientes casos:

   - pagos a favor de beneficiarios de confianza que estén incluidos en listas blancas que ese cliente haya establecido con anterioridad;
   - operaciones realizadas entre dos cuentas del mismo cliente dentro de un único PSP;
   - transferencias dentro del mismo PSP cuando esté justificado por un análisis del riesgo de las operaciones;
   - pagos de escasa cuantía, tal y como se definen en la DSP.[14]

   7.2 Para obtener acceso a los datos de pago sensibles o modificarlos (incluidas la creación y modificación de listas blancas) es necesaria una autenticación fuerte del cliente. Cuando un PSP ofrezca servicios de consulta sin que se visualice la información sensible del pago o del cliente, tales como datos de las tarjetas de pago que pudieran fácilmente emplearse para cometer fraude, el PSP podrá adaptar sus requisitos de autenticación en función de su evaluación de riesgos.

   7.3 [tarjetas] En el caso de las operaciones con tarjeta, todos los PSP emisores darán soporte a la autenticación fuerte del titular. Todas las tarjetas emitidas deberían estar técnicamente preparadas (registradas) para ser utilizadas con autenticación fuerte.

   7.4 [tarjetas] Los PSP que ofrezcan servicios de adquirencia estarán en disposición de soportar tecnologías que permitan al emisor realizar una autenticación fuerte del titular en los regímenes de pago con tarjeta en los que el adquirente participe.

[14] Véase la definición de los instrumentos de pago de escasa cuantía en el artículo 34, apartado 1, y el artículo 53, apartado 1, de la DSP.

7.5 [tarjetas] Los PSP que ofrecen servicios de adquisición deberían solicitar adquirencia solicitarán de sus respectivos comercios electrónicos que ofrezcan soluciones que permitan al emisor realizar la autenticación fuerte del titular para las operaciones de pago con tarjeta a través de internet. Se podría considerar el uso de medidas de autenticación alternativas para las categorías de operaciones previamente identificadas como de bajo riesgo tales como, por ejemplo, las basadas en un análisis de riesgos de las operaciones o las que implican pagos de escasa cuantía según se definen en la DSP.

7.6 [tarjetas] En los casos en que un determinado servicio acepte ciertos regímenes de pago con tarjeta, los proveedores de la solución tipo monedero solicitarán al emisor que exija la autenticación fuerte del titular legítimo, cuando este registre por primera vez los datos de la tarjeta.

7.7 Los proveedores de soluciones de pago tipo monedero permitirán que se pueda realizar la autenticación fuerte del cliente cuando este se identifique como usuario en los servicios de pago de tipo monedero o lleve a cabo operaciones con tarjeta a través de internet. Se podrá considerar el uso de medidas de autenticación alternativas para las operaciones de bajo riesgo previamente identificadas como, por ejemplo, las basadas en un análisis de riesgos de la operación, o las que implican pagos de escasa cuantía según se definen en la DSP.

7.8 [tarjetas] En el caso de las tarjetas virtuales, el registro inicial se realizará en un entorno seguro y de confianza[15]. Cuando la tarjeta virtual se emita en el entorno de internet, en el proceso de generación de datos se debería solicitar la autenticación fuerte del cliente.

7.9 Los PSP deberían garantizar una autenticación bilateral adecuada cuando se comuniquen con los comercios electrónicos con el propósito de iniciar pagos por internet y de acceder a datos de pago sensibles.

Registro y distribución de las herramientas de autenticación y/o de software a los clientes

8. Los PSP garantizarán que el registro del cliente y la distribución inicial de las herramientas de autenticación necesarias para utilizar el servicio de pago por internet, y/o del software relacionado con los pagos, se lleven a cabo de forma segura.

8.1 El registro y distribución al cliente de las herramientas de autenticación y/o la entrega al mismo de software relacionado con los pagos, cumplirán los siguientes requisitos:

[15] Los entornos bajo la responsabilidad del PSP en los que se garantiza una autenticación adecuada del cliente y del PSP que ofrece el servicio, así como la protección de información confidencial/sensible incluyen: i) las instalaciones del PSP; ii) la banca por internet u otro sitio web seguro, por ejemplo, cuando la autoridad de gobierno (GA, en sus siglas en inglés) ofrece características de seguridad comparables, entre otras, a las definidas en la Directriz 4; o iii) servicios de cajeros automáticos. (En el caso de los cajeros automáticos, se requiere la autenticación fuerte del cliente. Tal autenticación se realiza normalmente con chip y PIN, o con chip y una característica biométrica).

- Los procedimientos correspondientes se realizarán en un entorno seguro y de confianza, teniendo en cuenta los posibles riesgos derivados de los dispositivos que no están bajo el control del PSP.

- Se establecerán procedimientos efectivos y seguros para la entrega de las credenciales de seguridad personalizadas, el software relacionado con los pagos y todos los dispositivos personalizados asociados a los pagos por internet. El software entregado a través de internet deberá, además, estar firmado digitalmente por el PSP para permitir que el cliente pueda verificar su autenticidad y que este no haya sido falsificado.

- [tarjetas] En las operaciones con tarjeta, la adhesión por parte del cliente a los procedimientos de autenticación fuerte deberá estar disponible con independencia de si se realiza una compra específica en internet. Cuando se ofrezca la activación durante una compra en internet, esta se llevará a cabo redirigiendo al cliente a un entorno seguro y de confianza.

8.2 [tarjetas] Los emisores de tarjetas fomentarán activamente el alta del titular en los servicios de autenticación fuerte y permitirán que los titulares no se inscriban únicamente en casos excepcionales y limitados, y solo cuando estén justificados por el riesgo asociado a la operación específica con la tarjeta.

Intentos de inicio de sesión, tiempo límite de sesión, validez de la autenticación

9. Los PSP limitarán el número de intentos fallidos de inicio de sesión o de autenticación, definirán normas para el tiempo límite de inactividad de cada sesión de servicios de pago por internet y establecerán límites de tiempo para la caducidad de cada autenticación.

9.1 Cuando se use una contraseña de un solo uso (*one-time-password* u OTP, en sus siglas en inglés) para la autenticación, los PSP garantizarán que el periodo de validez de dichas contraseñas se limite a lo estrictamente necesario.

9.2 Los PSP establecerán el número máximo de intentos fallidos de conexión o de autenticación tras los cuales se bloqueará el acceso al servicio de pagos por internet (de forma temporal o permanente). Dispondrán de un procedimiento seguro para reactivar los servicios de pago por internet bloqueados.

9.3 Los PSP establecerán el periodo máximo tras el cual las sesiones inactivas de servicios de pago por internet finalizan de forma automática.

Seguimiento de las operaciones

10. Los mecanismos de seguimiento de las operaciones diseñados para evitar, detectar y bloquear operaciones de pago fraudulentas deberán activarse antes de que se obtenga la autorización final del PSP. Las operaciones sospechosas o de alto riesgo estarán sujetas a un

procedimiento de examen y evaluación específico. Además, se establecerán mecanismos de autorización y seguimiento de la seguridad equivalentes para la emisión de los mandatos electrónicos.

10.1 Los PSP usarán sistemas de prevención y detección de fraude para identificar operaciones sospechosas antes de que el PSP dé la autorización final a las operaciones o mandatos electrónicos. Dichos sistemas se basarán en, por ejemplo, reglas parametrizadas (tales como listas negras de tarjetas comprometidas o robadas), y controlarán los patrones de comportamiento anómalo del cliente o del dispositivo de acceso del cliente (como un cambio en la dirección IP[16] o en el rango IP durante la sesión de pagos por internet, a veces identificado mediante comprobación por geolocalización de la dirección IP[17], categorías atípicas de comercios electrónicos para un cliente específico, datos anómalos de las operaciones, etc.). Estos sistemas han de ser capaces también de detectar síntomas de infección por software malicioso en la sesión (por ejemplo, a través de comandos frente a una validación manual) y escenarios de fraude conocidos. El alcance, la complejidad y la adaptabilidad de las soluciones de seguimiento, cumpliendo con la legislación pertinente de protección de datos, serán proporcionales al resultado de la evaluación de riesgos.

10.2 Los PSP adquirentes dispondrán de sistemas de prevención y detección de fraude para controlar las actividades de los comercios electrónicos.

10.3 Los PSP llevarán a cabo los procedimientos de examen y evaluación de las operaciones dentro de un periodo de tiempo adecuado para no retrasar indebidamente el inicio y/o la prestación del servicio de pago pertinente.

10.4 Cuando el PSP, según su política de riesgo, decida bloquear una operación de pago que haya sido identificada como potencialmente fraudulenta, mantendrá el bloqueo durante el menor tiempo posible hasta que se solucionen los problemas de seguridad.

Protección de datos de pago sensibles

11. Los datos de pago sensibles se protegerán tanto durante su almacenamiento, como durante su procesamiento o transmisión.

11.1 Todos los datos usados para identificar y autenticar a los clientes (por ejemplo, al iniciar sesión, al iniciar pagos por internet y al emitir, modificar o cancelar mandatos electrónicos), así como la interfaz del cliente (sitio web del PSP o comercio electrónico) estarán protegidos de forma adecuada frente al robo y al acceso o modificación no autorizados.

[16] Una dirección IP es un código numérico único que identifica a cada ordenador conectado a Internet.

[17] Una comprobación «GeoIP» verifica si el país emisor se corresponde con la dirección IP desde la que el usuario inicia la operación.

11.2 Los PSP garantizarán que, al intercambiar datos de pago sensibles a través de internet, y a fin de proteger su confidencialidad e integridad, durante cada sesión de comunicación se aplicará el cifrado de extremo a extremo seguro [18] entre los intervinientes en ella, usando técnicas de cifrado fuerte y ampliamente reconocidas.

11.3 Los PSP que ofrezcan servicios de adquirencia promoverán que los comercios electrónicos no almacenen datos de pago sensibles. En caso de que los comercios electrónicos manejen, es decir, almacenen, procesen o transmitan datos de pago sensibles, dichos PSP les exigirán contractualmente que dispongan de las medidas necesarias para proteger estos datos. Los PSP llevarán a cabo comprobaciones periódicas y, cuando llegue a su conocimiento que un comercio electrónico que maneja datos de pago sensibles no cuenta con las medidas de seguridad necesarias, emprenderán acciones para exigir el cumplimiento de esta obligación contractual o para resolver el contrato.

[18] El cifrado de extremo a extremo hace referencia al cifrado en el terminal de origen, produciéndose la correspondiente descodificación únicamente en el terminal de destino. ETSI EN 302 109 V1.1.1. (2003-06).

Sensibilización, formación de los clientes y comunicación con los clientes

Formación de los clientes y comunicación con los clientes

12. Los PSP proporcionarán asistencia y orientación a los clientes, cuando sea necesario, en relación con el uso seguro de los servicios de pago por internet. Los PSP se comunicarán con sus clientes de forma que estos puedan confiar en la autenticidad de los mensajes recibidos.

12.1 Los PSP proporcionarán como mínimo un canal seguro[19] para una comunicación continua con los clientes en todo lo relativo al uso correcto y seguro del servicio de pagos por internet. Los PSP informarán a los clientes de este canal y explicarán que cualquier mensaje en su nombre a través de otros medios, como el correo electrónico, en relación con el uso correcto y seguro del servicio de pagos por internet, no será fiable. Los PSP deberán especificar:

- el procedimiento para que los clientes les informen de (presuntos) pagos fraudulentos, incidentes o anomalías sospechosos durante la sesión de servicios de pago por internet y/o posibles casos de ingeniería social[20];
- los pasos que darán a continuación, es decir, cómo responderán al cliente;
- cómo notificarán al cliente las (posibles) operaciones fraudulentas o la no iniciación de estas, o cómo advertirán al cliente sobre la existencia de ataques (por ejemplo, correos electrónicos de suplantación de identidad).

12.2 A través del canal seguro, los PSP mantendrán informados a los clientes sobre las actualizaciones de los procedimientos de seguridad en los servicios de pago por internet. Las alertas sobre riesgos emergentes significativos (por ejemplo, advertencias sobre casos de ingeniería social) también deberán transmitirse a través del canal seguro.

12.3 Los PSP también pondrán a disposición de los clientes un servicio de asistencia para preguntas, reclamaciones, solicitudes de ayuda y notificaciones de anomalías o incidentes respecto a los pagos por internet y servicios relacionados, e informarán adecuadamente a los clientes sobre cómo obtener dicha asistencia.

12.4 Los PSP pondrán en marcha programas de sensibilización y formación de clientes, diseñados para garantizar que estos entiendan, como mínimo, la necesidad de:

[19] Por ejemplo, un buzón de correo electrónico específico en el sitio web del PSP o un sitio web seguro.

[20] En este contexto, la ingeniería social hace referencia a las técnicas de manipulación de personas para obtener información (por ejemplo, mediante correos electrónicos o llamadas telefónicas), o de recuperación de información de las redes sociales, con el fin de cometer fraude o para obtener acceso no autorizado a un ordenador o red.

- proteger sus contraseñas, *tokens*, datos personales y demás datos confidenciales;

- gestionar de forma adecuada la seguridad del dispositivo personal (por ejemplo, el ordenador), mediante la instalación y actualización de componentes de seguridad (antivirus, cortafuegos, parches de seguridad);

- considerar las amenazas y riesgos significativos relacionados con la descarga de software a través de internet si el cliente no puede estar totalmente seguro de que el software es auténtico y no una falsificación;

- usar el sitio web legítimo que el PSP haya habilitado para efectuar pagos por internet.

12.5 Los PSP adquirentes solicitarán a los comercios electrónicos que separen claramente los procesos de pagos de los de compra en línea, para ayudar a los clientes a identificar cuándo se comunican con el PSP en lugar de con el beneficiario (por ejemplo, redirigiendo al cliente y abriendo una ventana nueva de forma que el proceso de pago no se muestre dentro del cuadro del comercio electrónico).

Notificaciones, establecimiento de límites

13. Los PSP establecerán límites para los servicios de pago por internet y proporcionarán a los clientes opciones para limitar aún más los riesgos dentro de dichos límites. También podrán prestar servicios de alertas y de gestión de perfiles de usuarios.

13.1 Antes de prestar al cliente servicios de pago por internet, los PSP establecerán límites[21] para estos servicios (por ejemplo, un importe máximo para cada pago individual o un importe acumulado para un periodo de tiempo determinado) e informarán de ello a sus clientes. Los PSP permitirán a los clientes desactivar la funcionalidad de pagos por internet.

Acceso de los clientes a la información sobre la iniciación del pago y su ejecución

14. Los PSP confirmarán a los clientes la iniciación del pago y les proporcionarán puntualmente la información necesaria para comprobar que una operación de pago se ha iniciado y/o ejecutado de forma correcta.

14.1 [transferencias/mandato electrónico] Los PSP proporcionarán a los clientes un servicio en tiempo cuasi real para comprobar, en cualquier momento[22] y en un entorno seguro y de confianza, tanto el grado de ejecución de las operaciones como los saldos de la cuenta.

[21] Tales límites podrán aplicarse de forma global (es decir, a todos los instrumentos de pago que permitan pagos por internet) o individualmente.

[22] Salvo por la falta de disponibilidad excepcional del servicio por motivos de mantenimiento técnico, o como resultado de incidentes graves.

14.2 Los estados electrónicos detallados se facilitarán en un entorno seguro y de confianza. Cuando los PSP informen a los clientes sobre la disponibilidad de los estados electrónicos (ya sea regularmente, cuando se emitan estados electrónicos periódicos, o *ad hoc* tras la ejecución de una operación) a través de un canal alternativo, como, por ejemplo, SMS, correo electrónico o carta, no se incluirán en estas comunicaciones datos de pago sensibles y, si se incluyeran, deberán estar ocultos.

Título III. Disposiciones finales y aplicación

15. Las presentes Directrices serán de aplicación a partir del 01.08.2015.

Anexo 1: Ejemplos de buenas prácticas

Además de los requisitos anteriores, las presentes Directrices describen algunas de las buenas prácticas que se recomienda adoptar, pero no se obliga a hacerlo, a los PSP y a los correspondientes participantes en el mercado. Para facilitar la consulta, se indican los capítulos a los que se refieren cada una de ellas.

Entorno general de control y seguridad

Gobernanza

BP1: La política de seguridad podría establecerse en un documento específico.

Control y mitigación de riesgos

BP2: Los PSP podrían proporcionar herramientas de seguridad (por ejemplo, dispositivos y/o navegadores personalizados con un nivel de seguridad adecuado) para proteger la interfaz del cliente frente al uso indebido o ataques (por ejemplo, los ataques para interceptar el navegador «*man in the browser*» o MiTB en sus siglas en inglés).

Trazabilidad

BP3: Los PSP que ofrezcan servicios de adquirencia podrían exigir contractualmente a los comercios electrónicos que almacenen información sobre pagos, que dispongan de procesos adecuados que faciliten su trazabilidad.

Medidas específicas de control y seguridad para los pagos por internet

Identificación inicial de los clientes e información

BP4: Los clientes podrían firmar un contrato específico de servicios con el PSP para llevar a cabo operaciones de pago por internet, en lugar de incluir los términos y condiciones en un contrato de servicios general más amplio.

BP5: Los PSP también podrían asegurarse de que se proporcionen a los clientes, a través de los medios adecuados (por ejemplo, folletos o sitios web), ya sea de forma continua o puntualmente, instrucciones claras y directas que les expliquen sus responsabilidades en relación con el uso seguro del servicio.

Autenticación fuerte de los clientes

BP6: [tarjetas] Los comercios electrónicos podrían apoyar la autenticación fuerte del titular por el emisor en las operaciones con tarjeta a través de internet.

BP7: Por motivos de comodidad para el cliente, los PSP podrían considerar el uso de una herramienta única de autenticación fuerte del cliente para todos los servicios de pago por internet. Esto podría aumentar la aceptación de la solución entre los clientes y facilitar su correcto uso.

BP8: La autenticación fuerte del cliente podría incluir elementos que vinculasen la autenticación a un importe y beneficiario específicos. Esto podría aumentar la seguridad y confianza de los clientes a la hora de autorizar los pagos. La solución tecnológica que permita vincular los datos de autenticación fuerte con los datos de las operaciones debería ser a prueba de manipulaciones.

Protección de datos de pago sensibles

BP9: Se recomienda a los comercios electrónicos que manejen datos de pago sensibles que formen adecuadamente al personal que gestione los casos de fraude y que actualicen esta formación periódicamente, para garantizar que el contenido continúa siendo relevante en un entorno de seguridad dinámico.

Formación de los clientes y comunicación con los clientes

BP10: Se recomienda a los PSP que ofrezcan servicios de adquirencia que organicen programas de formación para los comercios electrónicos sobre la prevención del fraude.

Notificaciones, establecimiento de límites

BP11: Dentro de los límites establecidos, los PSP podrían proporcionar a los clientes herramientas para gestionar los límites de los servicios de pago por internet en un entorno seguro y de confianza.

BP12: Sobre la base de sus políticas de gestión de riesgos, los PSP podrían establecer alertas para los clientes, por ejemplo, mediante llamadas por teléfono o SMS, en caso de operaciones de pago sospechosas o de alto riesgo.

BP13: Los PSP podrían permitir que los clientes especifiquen normas generales personalizadas como parámetros de su comportamiento respecto a los pagos por internet y servicios relacionados; por ejemplo, que los pagos solo se inicien en determinados países y que los iniciados en cualquier otro lugar se bloqueen, o que los clientes puedan incluir potenciales beneficiarios en listas negras o blancas.