Revista CESCO de Derecho de Consumo **Nº 13/2015**

http://www.revista.uclm.es/index.php/cesco **I. Estudios y Consultas**

PAGOS POR INTERNET: ¿RIESGOS A RAYA CON LAS DIRECTRICES DE SEGURIDAD PUBLICADAS POR LA AUTORIDAD BANCARIA EUROPEA?[1]

Mª Nieves Pacheco Jiménez

Prof. Contratada Doctora

Centro de Estudios de Consumo

Universidad de Castilla-La Mancha

Resumen: El avance de la tecnología facilita al consumidor numerosas tareas (con los consiguientes riesgos de mal manejo, fraudes o ataques cibernéticos), entre ellas los pagos por Internet, lo que supone la necesidad de los proveedores de servicios de pago de adaptarse a las nuevas circunstancias dadas en el entorno web. Se hace precisa una óptima intervención del legislador y de las autoridades competentes con la finalidad de fomentar un sistema de pago seguro que genere plena confianza al consumidor/usuario. Una muestra de ello viene dada por la Autoridad Bancaria Europea que, con sus directrices sobre seguridad en los pagos por Internet, realiza una serie de recomendaciones para asentar un estándar mínimo de seguridad. Este estudio contextualiza y analiza las mencionadas directrices, así como su impacto en el ámbito de la ciberseguridad.

Palabras clave: consumidor-usuario, ciberseguridad, pagos por Internet, Autoridad Bancaria Europea, directrices.

Title: Internet payments: what about cyber-risks after final guidelines on security issued by european banking authority?

Abstract: The technological advance helps the consumer to carry out several tasks (with consequent risks of mishandling, fraud or cyber attacks), including online

[1] Trabajo realizado en el marco del Proyecto de Investigación DER2011-28562, del Ministerio de Economía y Competitividad ("Grupo de Investigación y Centro de Investigación CESCO: mantenimiento de una estructura de investigación dedicada al Derecho de Consumo"), que dirige el Prof. Ángel Carrasco Perera.

payments. This would require payment services providers to adapt to new circumstances given on the website environment. It is necessary an optimal intervention by legislator and competent authorities in order to promote a secure payment system that generates consumer/user e-confident. An example of this is given by European Banking Authority and the final guidelines on the security of internet payments, configured as recommendations to set a minimum safety standard. This research contextualizes and analyzes these guidelines, as well as their impact in cybersecurity.

Keywords: consumer-user, cybersecurity, internet payments, European Banking Authority, guidelines.

SUMARIO: 1. Introducción: tecnología y seguridad cibernética. 2. La Autoridad Bancaria Europea en el ámbito del sistema de pagos por internet. 3. Directrices finales de la Autoridad Bancaria Europea sobre la seguridad de los pagos por internet. *3.1. Contenido del documento. 3.2. Resumen ejecutivo. Antecedentes y fundamento. 3.3. Directrices sobre la seguridad de los pagos por internet. 3.3.1. Introducción. 3.3.2. Título I. 3.3.3. Título II. 3.3.4. Anexo I. 3.4. Documentos de acompañamiento. 3.5. Formulario de confirmación de conformidad con las directrices y recomendaciones*. 4. Consideraciones finales.

1. Introducción: tecnología y seguridad cibernética

Como es fácilmente constatable, desde hace unos años estamos inmersos en un continuo avance tecnológico en el ámbito de los pequeños dispositivos electrónicos (*smartphones*, *tablets*) que facilitan muchas de nuestras labores cotidianas (v.gr., lectura de prensa, consulta de correo electrónico, visita de redes sociales, compra de productos y servicios *online*, Banca en línea).

Tras leer el informe que reúne los resultados de la encuesta de opinión pública "Especial Eurobarómetro" sobre "seguridad cibernética"[2] en los países de la UE27 y Croacia, no cabe la menor duda de que Internet no está exenta de riesgos. Obviamente ello repercute en la confianza del usuario en el denominado *e-comercio* (concretamente en la venta al por menor y en el sector bancario).

La referida encuesta, que examina la frecuencia y el tipo de uso que los ciudadanos de la UE realizan de Internet, su confianza en las transacciones *online*, su experiencia en ciberdelitos y el nivel de concienciación que tienen acerca de este tipo de delitos, arroja, entre otros, los siguientes resultados:

[2] Special Eurobarometer 404 – Cyber security, publicado en noviembre de 2013.

Vid. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

1) Los niveles de uso de Internet son muy dispares entre los países: mientras más de la mitad de los ciudadanos de la UE acceden al menos una vez al día (54%), una sustancial minoría (28%) afirma no acceder nunca[3].

2) Además de acceder a Internet desde un ordenador portátil o un *netbook* (62%), o un ordenador de sobremesa (53%), el 35% de los usuarios de Internet acceden a través de un *smartphone*[4], y el 14% utilizan una *tablet* o pantalla táctil.

3) Alrededor de la mitad de los usuarios de Internet en la UE dicen visitar redes sociales (55%), comprar productos o servicios *online* (50%) o realizar Banca *online* (48%), mientras que el 18% vender bienes o servicios[5].

4) Cuando el uso de Internet se dirige a banca o compras *online*, las preocupaciones[6] más comunes de los usuarios son que alguien pueda coger o usar inadecuadamente sus datos personales (37%) y la seguridad de los pagos (35%).

5) Un 10% de los usuarios de Internet en toda la UE ha experimentado fraude *online*, y un 6% robos de identidad. Un 12% no ha podido tener acceso a servicios *online* debido a ataques cibernéticos, y un 12% ha tenido una cuenta de correo electrónico hackeada. Por último, un 7% ha sido víctima de fraude de tarjeta de crédito o de Banca *online*.

6) Los usuarios de Internet han cambiado su comportamiento en lo relativo a la seguridad. Así, un 46% ha instalado un antivirus, un 40% no abre los *e-mails* de remitentes desconocidos, un 34% no da información personal en los sitios web, un 32% sólo visita los sitios web que conoce y en los que confía, un 26%

[3] Concretamente, y atendiendo a la tabla QC1 sobre la frecuencia de acceso a Internet (para enviar *e-mails*, leer noticias *online*, chatear o comprar productos *online*), un 50% de los usuarios españoles accede al menos una vez al día, un 11% al menos una vez a la semana, y un 1% al menos una vez al mes. Se sitúa así España en el puesto número 9 del ránking UE27 y Croacia, siendo la media de un 54%, un 13% y un 2% de los ítems citados. Suecia tendría en el porcentaje más alto de acceso al menos una vez al día (85%) y Rumanía el más bajo (35%). Asimismo, los porcentajes varían por edad y sexo, resultando que: un 59% de los hombres accede a Internet al menos una vez al día, frente a un 50% de las mujeres; los usuarios con edades comprendidas entre los 15-24 años y los 25-39 años son los que más acceden al menos una vez al día, respectivamente un 86% y un 74%.

[4] Atendiendo a la tabla QC2 sobre el tipo de dispositivo empleado para acceder a Internet, la proporción de usuarios que lo hacen vía *smartphone* varía considerablemente según el país: es mayor en Suecia (64%), Reino Unido (56%), Dinamarca (55%) y Países Bajos (51%), y menor en Bulgaria Polonia (11%), Bulgaria (12%), Rumanía (13%) y Portugal (13%). Por su parte, un 44% de los usuarios españoles acceden a través de su *smartphone*.

[5] Atendiendo a la tabla QC3 sobre el tipo de actividades realizadas *online*, los usuarios españoles se distribuyen del siguiente modo: 85% para leer sus *e-mails*, 60% para leer noticias *online*, 58% para redes sociales, 33% para Banca *online*, 29% para comprar productos o servicios, 18% para juegos *online*, 11% para ver televisión, 5% para vender productos y servicios.

[6] Atendiendo a la tabla QC4 sobre el grado de confianza en la Banca *online* o compra de productos o servicios, un 51% de los usuarios españoles tiene total confianza, encontrándose la media europea en un 70%.

sólo usa su propio ordenador, un 24% emplea diferentes contraseñas para diferentes sitios web, y un 6% afirma haber cancelado una compra *online* por sospechar del vendedor o del sitio web[7].

2. La Autoridad Bancaria Europea en el ámbito del sistema de pagos por internet

Pues bien, el escenario brevemente descrito hasta ahora requiere un mecanismo para reducir los riesgos en ciber-seguridad, siendo uno de los ámbitos más complejos el sistema de pagos realizados por Internet. Este método consiste en un conjunto de instrumentos, procedimientos bancarios y, habitualmente, sistemas de transferencias de fondos interbancarios que aseguran la circulación del dinero. Es cierto que los sistemas de pago eficientes reducen el coste del intercambio de bienes y servicios, son indispensables para el funcionamiento de los mercados interbancarios, de dinero y de capitales, y se configuran como un elemento esencial en la infraestructura bancaria. Sin embargo, los sistemas de pago débiles pueden suponer un impedimento para la estabilidad y el desarrollo de una economía, desarrollando riesgos compartidos entre los participantes en el mercado, y reduciendo la cofianza en el sistema financiero. Por tanto, y para evitar esta poco deseable situación, los legisladores deben promover la regulación de la eficiencia técnica de los sistemas de pago por Internet.

Con los antecedentes descritos, la Autoridad Bancaria Europea (en lo sucesivo EBA[8]) presentó a mediados de diciembre de 2014 una serie de directrices para mejorar la seguridad de los consumidores de la UE en sus compras a través de Internet con el objetivo de luchar contra el fraude *online* y aumentar la confianza de aquellos en los servicios de pago vía Internet. El acento de estas recomendaciones se pone en el inicio de los pagos –bien a través de servicios de Banca *online* bien mediante el uso de tarjetas- y en el acceso a datos sensibles, que deben protegerse a través de una fuerte autenticación de la identidad del cliente-usuario.

---

[7] Atendiendo a la table QC6 sobre los cambios realizados en el modo de usar Internet, el 33% de los usuarios españoles ha instalado un antivirus, un 37% no abre los emails de remitentes desconocidos, un 21% no da información personal en los sitios web, un 30% sólo visita los sitios web que conoce en los que confía, un 25% sólo utiliza su propio ordenador, un 20% empela diferentes contraseñas para diferentes sitios web, y un 2% ha cancelado una compra *online* por sospechar del vendedor o del sitio web.

[8] European Banking Authority: Autoridad independiente de la UE establecida el 1 de enero de 2011, que trabaja para garantizar una regulación eficaz y coherente, así como la supervisión del sector bancario europeo. Sus objetivos generales son: mantener la estabilidad financiera en la UE y salvaguardar la integridad, la eficiencia y el correcto funcionamiento del sector bancario. Su principal tarea es contribuir a la creación de un único código normativo europeo en Banca, cuya finalidad es proporcionar un conjunto único de normas armonizadas para las instituciones financieras en toda la UE. Además, desempeña un papel importante en la promoción de la convergencia de las prácticas supervisoras, debiendo evaluar los riesgos y vulnerabilidades en el sector bancario de la UE. *Vid*. www.eba.europa.eu

3. Directrices finales de la Autoridad Bancaria Europea sobre la seguridad de los pagos por internet

3.1. Contenido del documento

La EBA ha presentado las referidas directrices con el objetivo de que sean asumidas por los proveedores de servicios de pago de la UE desde el próximo 1 de agosto de 2015.

El documento publicado por la EBA consta de cinco capítulos:

1) Resumen ejecutivo.

2) Antecedentes y Fundamento.

3) Directrices sobre la seguridad de los pagos por Internet: 3.a. *Status* de las directrices. 3.b. Requisitos de notificación. 3.c. Directrices: Título I, "alcance y definiciones"; Título II, "directrices sobre la seguridad de los pagos por Internet" (control general y entorno de seguridad; control específico y medidas de seguridad para los pagos por Internet; confianza de los clientes, educación y comunicación); Anexo 1, "ejemplos de mejores prácticas".

4) Documentos de acompañamiento: 4.a. Análisis de coste-beneficio y valoración de impacto. 4.b. Puntos de vista del Grupo de Stakeholder Bancario[9]. 4.c. *Feedback* sobre la consulta pública.

5) Formulario de confirmación de conformidad con las directrices y recomendaciones.

3.2. Resumen ejecutivo. Antecedentes y fundamento

Estos dos capítulos, que contextualizan las directrices abordando sus antecedentes y objeto, pueden resumirse como prosigue:

- El 31 de enero de 2013, el Banco Central Europeo (BCE) publicó recomendaciones finales para la seguridad de los pagos por Internet. Dicha publicación siguió a una consulta pública de dos meses llevada a cabo en 2012, y representó el primer resultado sobre el pago seguro. En ese

[9] Banking Stakeholder Group (BSG): Se compone de 30 miembros nombrados para representar de manera equilibrada a entidades de crédito y de inversión que operan en la UE, los representantes de sus empleados, así como a consumidores, usuarios de servicios financieros, académicos y representants de PYMES. La labor del Grupo es facilitar la consulta con las partes interesadas en los ámbitos relacionados con las las funciones del EBA. En particular, el Grupo deberá ser consultado sobre las medidas relativas a las normas técnicas de regulación y a las normas técnicas de ejecución, así como sobre las directrices y recomendaciones, en la medida en que éstas no se refieran a entidades financieras individuales.

Vid. http://www.eba.europa.eu/about-us/organisation/banking-stakeholder-group

momento la fecha de aplicación de las citadas recomendaciones se estableció en el 1 de febrero 2015.

- Durante una revisión sobre la marcha de la ejecución en el verano de 2014, el Foro de Pago Seguro[10] concluyó que sería beneficiosa una base jurídica más sólida para garantizar una aplicación coherente por parte de las entidades financieras de los Estados miembros, así como para dotarlas de confianza. Para ello, la EBA, como miembro del Foro de Pago Seguro, decidió convertir las recomendaciones de éste en directrices, de conformidad con el art. 16 del la Reglamento EBA 1093/2010 del Parlamento Europeo y del Consejo de 24 de noviembre de 2010, con alguna modificación menor para que estuviesen en línea con la Directiva de Servicios de Pago[11].

- El 20 de octubre de 2014, la EBA publicó un Documento de Consulta con directrices para la seguridad de pagos por Internet, que se basaban en recomendaciones desarrolladas y publicadas por el Foro de Pago Seguro en enero de 2013. De este modo, la conversión en directrices de la EBA se realiza con la intención de proporcionar una base legal sólida para una aplicación coherente de los requisitos en los 28 Estados miembros.

- Dado que las negociaciones sobre la revisión de la Directiva de Servicios de Pago estaban en curso, el Documento de Consulta solicitó a las partes interesadas su punto de vista sobre cómo las normas de seguridad potencialmente mayores requeridas por la futura Directiva deberían ser atendidas por la EBA. Se presentaron dos opciones, pidiendo a los encuestados que expresasen su preferencia sobre si las directrices finales de la EBA en línea con la Directiva de Servicios de Pago deberían: a) entrar en vigor el 1 de agosto de 2015, con el contenido que figura en el Documento de Consulta, lo que conllevaría una aplicación transitoria hasta que requisitos más fuertes entrasen en vigor en una fecha posterior en el marco de la futura Directiva (esto es, un mecanismo de dos pasos); b) anticiparse a los mencionados requisitos fuertes y, una vez que las negociaciones sobre la futura Directiva concluyeran, incluirlos en las directrices finales sobre la base de la vigente Directiva, entrando en vigor

[10] European Forum on the Security of Retail Payments: Foro Europeo sobre Seguridad en Pagos Menores.

Se creó en 2011 como una iniciativa de cooperación voluntaria entre las autoridades. Su objetivo es facilitar el conocimiento y entendimiento común, en particular, entre los supervisores de los proveedores de servicios de pago sobre cuestiones relacionadas con la seguridad de los servicios de pequeños pagos electrónicos en el ámbito de la UE con la finalidad de establecer un nivel mínimo armonizado de seguridad.

[11] Directiva 2007/64/CE del Parlamento Europeo y del Consejo sobre Servicios de Pago en el mercado interior. Tiene como objetivo instaurar el marco jurídico necesario para la creación de un mercado de pagos integrado, en el que se suprimirán los impedimentos a la entrada de nuevos proveedores de servicios. Además, la Directiva pretende reforzar la competencia y ofrecer a los usuarios un mayor número de opciones. Por último, garantiza un nivel de protección elevado gracias a los requisitos en materia de información y a la definición de los derechos y obligaciones de los usuarios y de los proveedores de servicios de pago.

el 1 de agosto de 2015, y continuándose aplicando bajo el marco de la ulterior Directiva (mecanismo de un paso).

- El período de consulta se cerró el 14 de noviembre de 2014, recibiendo la EBA 45 respuestas al Documento de Consulta, incluyendo una respuesta del Grupo de Stakeholder Bancario. Pues bien, la mayor parte de esas respuestas se decantaron por el mecanismo de dos pasos.

- Tras la valoración de todas las respuestas, la EBA llegó a las siguientes conclusiones: En primer lugar, dado el alto nivel de fraude observado en los pagos por Internet y su tendencia creciente en los últimos años, considera que no es plausible la preferencia de los encuestados para retrasar la aplicación de las directrices hasta la oportuna transposición de la Directiva de Servicio de Pagos en 2017. En segundo lugar, las cifras de fraude en los pagos con tarjeta ponen de manifiesto que la falta de seguridad sigue minando la confianza de los participantes en el mercado de los sistemas de pago, siendo precisa una oportuna y coherente regulación al respecto. De ahí que la EBA termine publicando sus directrices finales con fecha de aplicación de 1 de agosto de 2015.

3.3. Directrices sobre la seguridad de los pagos por internet

3.3.1. Introducción

Las directrices exponen la línea de la EBA sobre las prácticas de supervisión apropiadas dentro del Sistema Europeo de Supervisión Financiera. La EBA espera el cumplimiento de aquellas por parte de todas las autoridades competentes y de las entidades financieras a las que van dirigidas. Es más, las autoridades competentes deberán notificar a la EBA el cumplimiento o intención de cumplimiento de las mencionadas pautas, o de las razones para su no cumplimiento, en el plazo de dos meses desde la publicación de las traducciones de aquellas.

El capítulo relativo a las directrices en sentido estricto se estructura en: Título I, "Alcance y definiciones"; Título II, "Directrices sobre la seguridad de los pagos por Internet" (control general y entorno de seguridad; control específico y medidas de seguridad para los pagos por Internet; confianza de los clientes, educación y comunicación); Anexo 1, "ejemplos de mejores prácticas".

3.3.2. Título I

El Título I recoge, en primer lugar, el alcance de las directrices, estableciendo que se trata de un conjunto de requisitos mínimos en el ámbito de la seguridad de los pagos por Internet. Así, se basan en las normas de las Directiva 2007/64/CE, sobre Servicios de Pago, concernientes a la obligación de información y a las obligaciones de los proveedores de servicios de pagos en relación a la provisión de los

referidos servicios. Además, el art. 10.4 de la Directiva emplaza a las entidades de pago a tener un acuerdos de gobernanza sólidos y mecanismos de control interno adecuados. Se dirigen a las entidades financieras definidas en el art. 4.1 del Reglamento 1093/2010 y a las autoridades competentes del art. 4.2 de la misma norma. Estas últimas podrán requerir a los proveedores de servicios de pago notificar el cumplimiento de las directrices.

Es cierto que estas pautas finales constituyen unos requisitos mínimos para los servicios de pago por Internet (v. gr., tarjetas, tarjetas virtuales, transferencias, domiliación electrónica, dinero electrónico)[12], independientemente del dispositivo de acceso empleado. De ahí que aquellas se observen sin perjuicio de la responsabilidad de los proveedores de servicios de pago para supervisar y evaluar los riesgos en sus operaciones, desarrollar sus propias políticas de seguridad e implementar la seguridad, la gestión de incidencias y las medidas de continuidad del negocio.

En segundo lugar, el Título I establece una serie de definiciones adicionales a las previstas en la Directiva de 2007. A saber:

a) "Autenticación": procedimiento que permite al proveedor se servicios de pago verificar la identidad de un cliente.
b) "Autenticación fuerte de cliente": procedimiento basado en el uso de dos o más de los siguiente elementos: algo que sólo el usuario sabe (v. gr., contaseña estática, código, número de identificación personal); algo que sólo el usuario posee (v. gr., ficha, tarjeta inteligente, telefóno móvil); algo que el usuario es (v. gr., característica biomética, como una huella dactilar). Además, los elementos seleccionados deben ser independientes entre sí, de modo que el incumplimiento de uno no ponga en peligro el otro. Y al menos uno de los elementos debe ser de un solo uso, no replicable y no susceptible de ser robado subrepticiamente a través de Internet. En definitiva, el procedimiento de autenticación fuerte debe ser diseñado para proteger la confidencialidad.
c) "Autorización": procedimiento que comprueba si un cliente o un proveedor de servicios tiene derecho a realizar una acción

[12] Quedarían excluidos de su ámbito de aplicación: otros servicios de Internet prestados por un proveedor de servicios de pago a través de su propia web de pago (v. gr., corretajes, contratos en línea); pagos en los que la insgrucción se da por correo, teléfono, correo de voz o SMS; pagos móviles distintos de los pagos basados en el navegador; transferencias en las que un tercero acceda a la cuenta de pago del cliente; operaciones de pago efectuadas por una empresa a través de redes especializadas; pagos con tarjeta empleando tarjetas prepago físicas o virtuales anónimas y no recargables, donde no existe relación continua entre el emisor y el titular de la tarjeta; compensación y liquidación de operaciones de pago.

determinada (v. gr., transferir fondos, tener acceso a datos sensibles).

d) "Credenciales": información –generalmente confidencial- proporcionada por un cliente o un proveedor de servicios para fines de autenticación. Pueden consistir en un instrumento físico que contiene la información (v. gr, tarjeta inteligente) o algo que el usuario memoriza o representa (v. gr., características biométricas).
e) "Incidente importante de seguridad de pago": incidente que tenga o pueda tener un impacto significativo en la seguridad, la integridad o la continuidad de los sistemas de pago de los proveedores de servicios y/o en la seguridad de los datos de pago sensibles o fondos. Para valorarse deben tenerse en cuenta el número de clientes potencialmente afectados, la cantidad en riesgo y el impacto en otros proveedores u otras infraestructuras de pago.
f) "Análisis de riesgo de la transacción": la evaluación del riesgo relacionado con una transacción específica teniendo en cuenta criterios tales como los patrones de pago del cliente, el valor de la transacción, el tipo de producto y el perfil del beneficiario.
g) "Tarjetas virtuales": solución de pago basada en una tarjeta donde se genera un número de tarjeta temporal con un período de validez reducido, un uso limitado y un límite de gasto preestablecido que puede ser utilizado para compras por Internet.
h) "Soluciones *wallet*": soluciones que permiten a un cliente registrar datos en relación con uno o más instrumentos de pago con el fin de realizar pagos con varios comerciantes electrónicos (v. gr., monedero electrónico).

3.3.3. Título II

El Título II establece las directrices sobre la seguridad de los pagos por Internet, estructurándose en varios apartados: A) Control general y seguridad del entorno. B) Control específico y seguridad de las medidas de pago por Internet. C) Concienciación del cliente, educación y comunicación.

A) Control general y seguridad del entorno

En este apartado se observan medidas referentes a la gobernanza, valoración de riesgos, supervisión y notificación de incidentes, control y minoración de riesgos, y seguimiento.

En lo referente a la gobernanza, los proveedores de servicios de pago deberán implementar y revisar periódicamente la política de seguridad de los servicios de pago por Internet. Así, la política de seguridad debe estar debidamente documentada, definir roles y responsabilidades, incluyendo la gestión de los datos de pago sensibles en relación con la evaluación de los riesgos, control y minoración.

En cuanto a la valoración de riesgos, los proveedores de servicios deben llevar a cabo y documentar las evaluaciones de los riesgos atendiendo a la seguridad de los pagos por Internet, tanto antes de establecer el servicio como después. Para ello habrán de considerarse: las soluciones tecnológicas utilizadas, los servicios subcontratados a proveedores externos y el entorno técnico de los clientes. Es esencial que la valoración se dirija a la necesidad de proteger y asegurar los datos sensibles de pago. Sobre esta base, los proveedores deberán determinar si son precisos cambios en las medidas de seguridad existentes, en las tecnologías utilizadas o en los servicios ofrecidos, debiendo prever el tiempo necesario para hacer efectivos dichos cambios. Además, y antes de un cambio relevante en la infraestructura o en los procedimientos, los proveedores deben realizar una revisión de los escenarios de riesgo y de las medidas de seguridad existentes después de los incidentes importantes que afecten a sus servicios. No obstante, una revisión general de la evaluación del riesgo debería efectuarse al menos una vez al año. Por último, los resultados de las evaluaciones de riesgos y revisiones deben presentarse a la alta dirección para su aprobación.

En lo relativo a la supervisión y notificación de incidentes, los proveedores de servicios de pago han de garantizar la vigilancia, el manejo y el seguimiento de manera coherente e integrada, incluyendo quejas de los clientes sobre seguridad. De ahí que aquellos deban establecer un procedimiento para notificar inmediatamente tales incidencias a la administración y, en caso de incidentes de seguridad importantes, a la autoridades competentes.

Sobre el control y minoración de riesgos, los proveedores de servicios de pago deben implementar medidas de acuerdo con sus respectivas políticas de seguridad con el fin de mitigar lo riesgos identificados. Así, estas medidas deberían incorporar múltiples capas de defensas de seguridad. Entre otras medidas se encontrarían las siguientes:

- En el diseño, desarrollo y mantenimiento de los servicios de pago por Internet, se debe prestar especial atención a la adecuada segregación de funciones en información de tecnología de entornos (v. gr., entornos de desarrollo, prueba y producción).
- Se deben tener soluciones de seguridad apropiadas para proteger redes, sitios web, servidores y enlaces de comunicación contra abusos o ataques.
- Se deben tener procesos adecuados para supervisar, controlar y restringir el acceso a los datos de pago sensibles, a los recursos críticos (v. gr., redes, sistemas, bases de datos, módulos de seguridad). Así, los proveedores deberían crear, almacenar y analizar los registros y pistas de auditoría.
- En el diseño, desarrollo y mantenimiento de los servicios de pago, se debe garantizar que la política de almacenamiento de datos es un componente esencial del la funcionalidad principal.

- Se deben probar periódicamente las medidas de seguridad, incluyendo escenarios de ataques potenciales relevantes y conocidos.
- Siempre que los proveedores externalicen funciones relacionadas con la seguridad de los servicios de pago por Internet, el contrato deberá incluir disposiciones que exijan el cumplimiento de los principios establecidos en las presentes directrices.

Finalmente, en lo concerniente al seguimiento, los proveedores de servicios de pago deben garantizar que todas las transacciones se siguen convenientemente. Eso significa que se deberían incorporar mecanismos de seguridad para el registro detallado de las transacciones, incluyendo el número secuencial, las marcas de tiempo de los datos, los cambios de parametrización, así como el acceso a los datos de la transacción y de domiciliación electrónica.

B) Control específico y medidas de seguridad para los pagos por Internet

En este apartado se observan medidas referentes a la identificación inicial del cliente e información; a la autenticación fuerte del cliente; al registro para –y provisión de- herramientas de autenticación y/o *software* entregado al cliente; a los intentos de inicio de sesión, el tiempo de espera de sesión y la validez de la autenticación; a la supervisión de la transacción y a la protección de datos de pago sensibles.

En lo atinente a la identificación inicial del cliente e información, se debe garantizar una identificación correcta acorde con la legislación europea contra el lavado de dinero, confirmándose la voluntad del cliente de hacer pagos por Internet utilizando los servicios antes de concederse el acceso a los mismos. Los proveedores de servicios deben proporcionar una información previa, regular y, en su caso, "ad hoc" acerca de los requisitos necesarios para la realización de transacciones de pago seguro por Internet y de los riesgos inherentes. Entre los elementos enumerados se encuentran los siguientes:

- información clara sobre requisitos tales como equipo de cliente, *software* u otras herramientas necesarias (v. gr., antivirus, cortafuegos);
- recomendaciones para el uso correcto y seguro de las credenciales de seguridad personalizadas;
- descripción paso a paso del procedimiento para solicitar y autorizar una operación de pago y/o recibir información, incluyendo las consecuencias de cada acción;
- pautas para el uso adecuado y seeguro de todo el *hardware* y *software* proporcionado al cliente;

- procedimientos a seguir en caso de pérdida o robo de las credenciales de seguridad personalizadas o *hardware* o *software* del cliente para poder acceder o realizar transacciones;
- procedimientos a seguir si se detecta o sospecha de un abuso;
- descripción de las responsabilidades y obligaciones de proveedor y cliente con respecto a la utilización de servicios de pago por Internet.
- posibillidad, en base al contrato marco con el cliente, del proveedor de bloquear una transacción específica o un instrumento de pago por problemas de seguridad[13].

En cuanto a la autenticación fuerte del cliente, se hace especial hincapié en la protección del cliente en el momento inicial de los pagos, así como en el acceso a los datos especialmente sensibles. Pueden señalarse, entre otras, las siguientes medidas:

- Para transferencias, domiciliaciones y dinero electrónico, los proveedores deben realizar la referida autenticación para la autorización del cliente de operaciones. No obstante, podrían adoptar medidas alternativas de autenticación para pagos salientes a beneficiarios de confianza incluidos en listas blancas previamente establecidas, transacciones entre dos cuentas del mismo cliente mantenidas en el mismo proveedor, pagos de bajo valor, etc.
- Para operaciones con tarjeta, todos los proveedores emisores de tarjetas deben dar soporte a una fuerte autenticación del titular de las mismas. Así, todas las tarjetas emitidas deben estar técnicamente preparadas para ser utilizadas con dicha autenticación.
- Para hacer efectiva la referida autenticación, los proveedores deben exigir a sus e-comerciantes que aporten soluciones que permitan al emisor realizar aquella.
- Para las operaciones con soluciones *wallet* los proveedores de éstas deben requerir autenticación fuerte cuando el titular legítimo registra por primera vez los datos de la tarjeta.
- Para las tarjetas virtuales, el registro inicial debe hacerse en un entorno seguro y de confianza.

En lo referente al registro para –y provisión de- herramientas de autenticación y/o *software* entregado al cliente, los proveedores de servicios de pago deben cumplir los siguientes requisitos:

- Los procedimientos han de desarrollarse en un entorno seguro y de confianza, teniendo en cuenta los posibles riesgos derivados de los dispositivos que no están bajo el control del proveedor.
- Los procedimientos eficaces y seguros deben estar en orden para la entrega de credenciales personalizadas de seguridad, *software* de pago y todos los dispositivos relacionados con pagos por Intenet. Es más, el *software* entregado a través de Intenet también debe ser

[13] Deben concretarse los métodos y términos en los que el cliente puede contactar con el proveedor de servicos para desbloquear la transacción o servicio.

firmado digitalmente por el proveedor para que el cliente compruebe su autenticidad y que no ha sido manipulado.

- Para las transacciones con tarjeta, cuando se ofrezca la activación de registro de datos con autenticación fuerte, se debe redirigir al cliente a un entorno seguro y de confianza.
- Los emisores de tarjetas deben fomentar activamente la inscripción de su titular para la autenticación fuerte, permitiendo pasar por alto dicha inscripción sólo en un número excepcional y limitado de casos, justificándose en el riesgo relacionado con la específica transacción.

En lo que concierne a los intentos de inicio de sesión, el tiempo de espera de sesión y la validez de la autenticación, los proveedores de servicios de pago han de considerar los siguientes aspectos:

- Al utilizarse una contraseña de un solo uso, es preciso asegurarse de que su período de validez se limita al mínimo estrictamente necesario.
- Establecerse el número máximo de intentos de inicios de sesión erróneos o de autenticación, bloqueándose después el acceso al servicio de pago por Internet (temporal o permanentemente); teniendo los proveedores un procedimiento seguro para reactivar el referido servicio.
- Se debe fijar el tiempo máximo tras el cual las sesiones inactivas terminan automáticamente.

Los mecanismos destinados a prevenir, detectar y bloquear las operaciones de pago fraudulentas deben ser ejecutados antes de la autorización final del proveedor. Asimismo, las transacciones sospechosas o de elevado riesgo deben ser objeto de un examen específico y procedimiento de evaluación. Los citados mecanismos deberían basrse, por ejemplo, en reglas parametrizadas (v. gr., listas negras de datos robados) o en patrones de comportamiento anormales (v. gr., cambio de protocolo de Intenet, datos de transacciones extraños). Además, estos sistemas también deberían ser capaces de detectar signos de infección de *malware* en la sesión y escenarios de fraude conocidos. Lógicamente, el alcance, complejidad y capacidad de adaptación de las soluciones de supervisión deben estar en consonancia con los resultados de la evaluación de riesgos y respetar la legislación pertinente sobre protección de datos.

Por último, los datos sensibles de pago deben ser protegidos en su almacenamiento, procesamiento y transmisión. De ahí que todos los datos utilizados para identificar y autenticar a los clientes deban ser convenientemente asegurados contra robo y acceso no autorizado o modificación. El intercambio de datos a través de Internet deberá hacerse de manera encriptada empleando ténicas sólidas y ampliamente reconocidas. En caso de que los proveedores utilicen servicios de adquisición, deben exhortar a sus e-comerciantes a no almacenar esos datos sensibles; si así lo hiciesen, aquellos deberan

exigirles contractualmente las medidas necesarias para proteger dichos datos, asegurándose de que se cumplen bajo sanción de rescindir el contrato.

C) Concienciación del cliente, educación y comunicación

En este apartado se observan medidas referentes a educación del cliente y comunicación, notificaciones y establecimiento de límites, acceso del cliente a información sobre el estado de inicio del pago y ejecución.

En cuanto a la educación del cliente y comunicación, los proveedores deben proporcionar asistencia y orientación, cuando sea necesario, sobre el uso seguro de los servicios de pago por Intenet. Además, la comunicación con los clientes debe realizarse de manera que se asegure la autenticidad de los mensajes recibidos. En base a ello:

- Se debe proporcionar al menos un canal seguro (v. gr., un buzón de correo en el sitio web del proveedor) para la comunicación con los clientes respecto al uso correcto y seguro del servicio de pago, explicándose que los mensajes en nombre del proveedor por cualquier otro medio no es fiable.
- Se debe explicar el procedimiento para que los clientes informen de presuntos pagos fraudulentos, incidentes o anomalías sospechosas durante la sesión de Internet, y de posible "ingeniería social" (técnicas de manipulación para obtener información a través de e-mail, llamadas telefónicas o redes sociales); así como el sistema de notificación por parte del proveedor al cliente de posibles transacciones fraudulentas o de advertencias de no inicio o de ataques de suplantación de identidad.
- A través del canal seguro, se debe mantener a los clientes informados de las actualizaciones en los procedimientos de seguridad en relación con los servicios de pago por Internet, así como de las alertas sobre riesgos emergentes importantes.
- Se debe poner a disposición del cliente un servicio de asistencia para preguntas, quejas, solicitudes de ayuda y notificaciones de anomalías o incidentes.
- Se deben iniciar programas de educación y sensibilización diseñadas para asegurar que el cliente comprenda, como mínimo, la necesidad de: proteger sus contraseñas, fichas de seguridad, datos personales y demás datos confidenciales; gestionar adecuadamente la seguridad del dispositivo personal a través de la oportuna instalación y actualización de componentes de seguridad (v. gr., antivirus, cortafuegos, parches de seguridad); tener en cuenta las amenazas y riesgos significativos relacionados con la descarga de *software* a través de Internet cuando el cliente no pueda estar razonablemente seguro de que aquel es original y no ha sido manipulado; utilizar el sitio web de pago genuino del proveedor.

Respecto a las notificaciones y establecimiento de límites, los proveedores deben fijar restricciones para los servicios de pago por Internet y ofrecer a sus clientes opciones para una mayor limitación del riesgo. Para ello se pueden ofrecer servicios de gestión de alertas y de perfiles de clientes, determinar una cantidad máxima por pago individual o una cantidad acumulada durante un determinado período de tiempo, así como permitir a los clientes deshabilitar la funcionalidad de pagos por Internet.

Finalmente, en lo que atañe al acceso del cliente a información sobre el estado de inicio del pago y ejecución, los proveedores han de proporcionar a sus clientes un servicio casi en tiempo real para comprobar el estado de la ejecución de las operaciones, así como los saldos de cuenta en cualquier momento en un ambiente seguro y de confianza. Asimismo, las declaraciones electrónicas deben expedirse regularmente o sobre una base *ad hoc* después de la ejecución de una transacción, no debiendo incluirse datos de pago sensibles (o si se hace, aparecer enmascarados).

3.3.4. Anexo I

En el Anexo I se consignan ejemplos de buenas prácticas para proveedores de servicios de pago y participantes en el e-mercado, caracterizándose por ser recomendaciones y no requisitos exigibles. Se trata de trece buenas prácticas en los concretos apartados de control general y control específico, destacando los siguientes consejos:

- La política de seguridad podría ser establecida en un documento específico.
- Los proveedores podrían proporcionar herramientas de seguridad (v. gr., dispositivos y/o navegadores personalizados, debidamente garantizados) para proteger la interfaz del cliente contra el uso ilegal o ataques.
- El cliente podría firmar un concreto contrato de un servicio para la realización de transacciones de pago por Internet, en lugar de los términos que se incluyen en un contrato de servicio general con el proveedor.
- Los proveedores podrían cerciorarse de que los clientes reciben instrucciones claras y sencillas que explican sus responsabilidades con respecto al uso seguro de su servicio.
- Por razones de conveniencia del cliente, los proveedores podrían considerar el uso de una sola herramienta de autenticación fuente para todos los servicios de pago por Internet. Esto podría aumentar la aceptación de la solución entre los clientes, así como facilitar un uso adecuado.
- Es deseable que los e-comerciantes que manejan datos de pago de carácter sensible formen a su personal sobre gestión del fraude, actualizando esta formación con regularidad para asegurar que el

contenido sigue siendo relevante para un entorno de seguridad dinámica.

3.4. Documentos de acompañamiento

Este capítulo complementa el documento de directrices con un análisis de coste-beneficio y valoración de impacto, con los puntos de vista del Grupo de Stakeholder Bancario[14] y con un *feedback* sobre la consulta pública.

El análisis de coste-beneficio y valoración de impacto repite básicamente lo señalado en el resumen ejecutivo, los antecedentes y el fundamento de las directrices, configurándose éstas como una serie de recomendaciones armonizadas y con carácter de mínima seguridad en la lucha contra el fraude en el pago, con la finalidad de aumentar la confianza del consumidor en los servicios de pago por Internet.

En cuanto al Grupo de Stakeholder Bancario, se indica cómo éste observó la necesidad de proporcionar una base jurídica sólida para la protección de los consumidores en el ámbito de la seguridad de los pagos por Internet, en lugar de depender de los acuerdos voluntarios existentes hasta la fecha. De hecho, un especial énfasis se puso en una mejor información al consumidor sobre los incidentes de seguridad, así como en la notificación de estos a las autoridades competentes. Asimismo, el Grupo solicitó expresamente un mecanismo de seguimiento para la aplicación de las directrices.

Por su parte, la EBA, tras las recomendaciones del Grupo, le recuerda la existencia de una guía de evaluación de la seguridad de los pagos por Internet, publicada por el Foro de Pago Seguro en febrero de 2014, cuyo objeto es ayudar a las autoridades nacionales competentes para evaluar el cumplimiento de las directrices por las entidades financieras.

Por último, respecto al denominado *feedback* sobre la consulta pública, realizada desde el 20 de octubre al 14 de noviembre de 2014, relativa a la materialización de las directivas en uno o dos pasos, se presenta un resumen de los puntos clave sobre las respuestas recibidas. Para mayor claridad al final del capítulo se adjunta una tabla con los siguientes ítems: pregunta, resumen de las respuestas, réplica de la EBA y enmiendas a las propuestas.

[14] Banking Stakeholder Group (BSG): Se compone de 30 miembros nombrados para representar de manera equilibrada a entidades de crédito y de inversión que operan en la UE, los representantes de sus empleados, así como a consumidores, usuarios de servicios financieros, académicos y representants de PYMES. La labor del Grupo es facilitar la consulta con las partes interesadas en los ámbitos relacionados con las las funciones del EBA. En particular, el Grupo deberá ser consultado sobre las medidas relativas a las normas técnicas de regulación y a las normas técnicas de ejecución, así como sobre las directrices y recomendaciones, en la medida en que éstas no se refieran a entidades financieras individuales.

Vid. http://www.eba.europa.eu/about-us/organisation/banking-stakeholder-group

3.5. Formulario de confirmación de conformidad con las directrices y recomendaciones

El documento de la EBA finaliza con un formulario de conformidad con las directrices y recomendaciones en el que, en primer lugar, se han de consignar los siguientes datos: fecha, Estado miembro, autoridad competente, directrices/recomendaciones, nombre, puesto, número de teléfono y correo electrónico. En segundo lugar se debe marcar: a) si se está autorizado para confirmar el cumplimiento de las directrices/recomendaciones en nombre de la autoridad competente y si la autoridad competente cumple o intenta cumplir las directrices y recomendaciones (dándose la opción de cumplimiento parcial). Acto seguido, y en caso de que la autoridad competente no cumpla, no intente cumplir o lo haga parcialmente, se han de señalar las razones. Por último, se indica que la notificación debe enviarse a la siguiente dirección de corre electrónico: complicance@eba.europa.eu, advirtiendo que otro sistema de comunicación no será aceptado como válido.

4. Consideraciones finales

Las previsiones de expertos en servicios y aplicaciones de pago a través de diferentes dispositivos son bastante favorables para el 2015[15]. De hecho, este año se presenta como el momento en que el teléfono puede relegar a la tarjeta bancaria como instrumento de pago por excelencia.

Ello pone de manifiesto la compleja relación entre tecnología, consumidores/usuarios, proveedores de servicios de pago, legislador y autoridades competentes. Así, el avance de la tecnología facilita al consumidor numerosas tareas (con los consiguientes riesgos de mal manejo, fraudes o ataques cibernéticos), entre ellas los pagos por Intenet, lo que supone la necesidad de los proveedores de servicios de pago de adaptarse a las nuevas circunstancias dadas en el entorno web. Y es aquí donde se hace precisa una óptima intervención del legislador y de las autoridades competentes con la

[15] Según iZettle, el proveedor líder europeo de servicios y aplicaciones de pago a través del móvil, habrá 2500 millones de usuarios de smartphones en 2015.

Vid. http://www.marketingdirecto.com/especiales/mobile-marketing-blog/4-previsiones-para-los-pagos-moviles-en-2015-segun-izettle/

Es más, para 2015 se prevé un crecimiento de los pagos por móvil del 60,8 por ciento.

Vid. http://ecommerce-news.es/servicios/metodos-de-pago/el-volumen-de-s-pagos-moviles-crecera-un-608-en-2015-18476.html

Asimismo, el nuevo DNI electrónico *3.0* incorpora un chip certificado como dispositivo seguro de mayor capacidad y velocidad que permite la transmisión de datos vía NFC (*Near Field Communication*; tecnología de comunicación inalámbrica) y la lectura sin PIN, lo que facilita su uso en *smartphones* y *tablets*, pudiendo pagar tasas a la Administración, entre otras funciones.

finalidad de fomentar un sistema de pago seguro que genere plena confianza al consumidor/usuario.

Si bien las directrices finales sobre seguridad en los pagos por Internet, publicadas por la Autoridad Bancaria Europea en el marco de la Directiva de Servicios de Pago de 2007 (aunque existe ya una propuesta –publicada en 2013- de ulterior Directiva acorde con los últimos avances en la materia) tras numerosos estudios sobre los riesgos inherentes a ese sistema de pago, son loables, al configurarse como meras recomendaciones para asentar un estándar mínimo de seguridad, no gozan de la deseable influencia atendiendo a la relevancia de los problemas que han surgido, surgen y seguirán surgiendo en un ámbito en continuo movimiento como es el de Internet. ¿Habrá entonces que esperar a la próxima Directiva sobre Servicios de Pago?