MEDIOS DE PAGO, SEGURIDAD E IDENTIDAD DIGITAL

Eduardo AVENDAÑO
David PÉREZ LÁZARO
Bárbara QUEIZÁN
Accenture Strategy

Resumen

En este artículo se realiza un análisis sobre el nuevo entorno de los medios de pago y la influencia de la era digital en los mismos en términos de emergencia de nuevas soluciones y nuevos competidores, pero también de nuevos retos relacionados con la seguridad y la identidad digital. En un mundo en el que los pagos por Internet y móviles están desplazando a los pagos tradicionales, es necesario que las entidades financieras y, en general, el conjunto de actores del ecosistema de pagos reflexione sobre cómo minimizar las amenazas en las transacciones y en la suplantación de la identidad del usuario en la ejecución del pago.

Palabras clave: pagos, móvil, Internet, seguridad, identidad digital.

Abstract

This paper presents an analysis of the new payments environment and the influence of the digital era as new solutions and new competitors arise, but also the new challenges related to security and digital identity. In a world where online and mobile payments are displacing traditional payments, it is necessary for financial institutions and, in general, the set of actors of the payment ecosystem, to think over on how to minimize transactions threats and impersonation of the digital identity in payments.

Key words: payments, mobile, internet, security, digital identity.

JEL classification: E42, G21.

I. EL NUEVO ENTORNO DE LOS MEDIOS DE PAGO

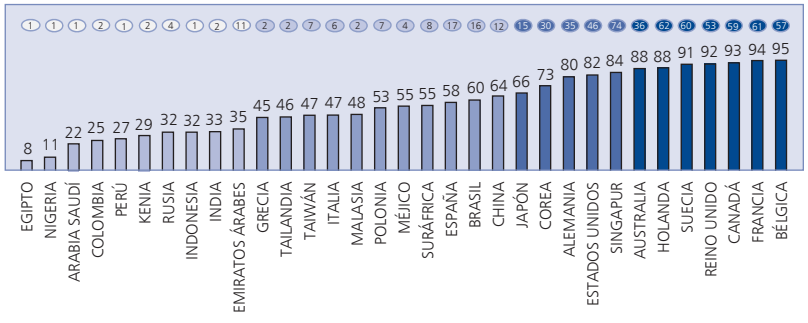
1. Hacia una economía sin efectivo

El dinero físico ha sido y sigue siendo el medio de pago más utilizado por particulares y comercios. Se estima que el 85 por 100 de las transacciones que se realizan en el mundo se efectúan en efectivo y que representan, aproximadamente, el 60 por 100 del valor de las mismas. No obstante, las cifras demuestran que los países confluyen paulatinamente hacia un entorno sin efectivo.

El ritmo de conversión es desigual en las diferentes geografías, si bien los gobiernos y entidades financieras de las economías más avanzadas están tomando decisiones encaminadas a reducir el uso de billetes y monedas como medida para paliar el fraude fiscal, facilitar la detección de movimientos financieros irregulares y eliminar la falsificación de dinero.

Algunos de los ejemplos más recientes en los que se han lanzado diferentes iniciativas en este sentido se encuentran en los países nórdicos. En Noruega, los bancos del país no distribuyen ni aceptan dinero en metálico en la mayoría de sus sucursales; en Suecia e Islandia se promueve la desaparición del dinero físico con la aplicación de medidas que permiten abonar con tarjeta cualquier compra, independientemente del importe; y

GRÁFICO 1
PENETRACIÓN INTERNACIONAL DE PAGOS EN EFECTIVO *VERSUS* NO EFECTIVO (% VOLUMEN DE TRANSACCIONES Y % VALOR DE TRANSACCIONES; 2014)



Fuentes: The Global Journey From Cash to Cashless, 2013 Mastercard; Proyección de datos 2014 Accenture.

en Dinamarca, desde enero de 2016, los comercios pueden negarse a aceptar pagos en efectivo, siendo la tendencia de uso de la tarjeta tan acusada que el Banco Central danés ha anunciado el cese de la producción de billetes y monedas. Por un lado, estas sociedades ganan en menor criminalidad y una creciente propensión al consumo, pero, por otro, las críticas se centran en la amenaza a la privacidad, la potencial exclusión social y la vulnerabilidad tecnológica.

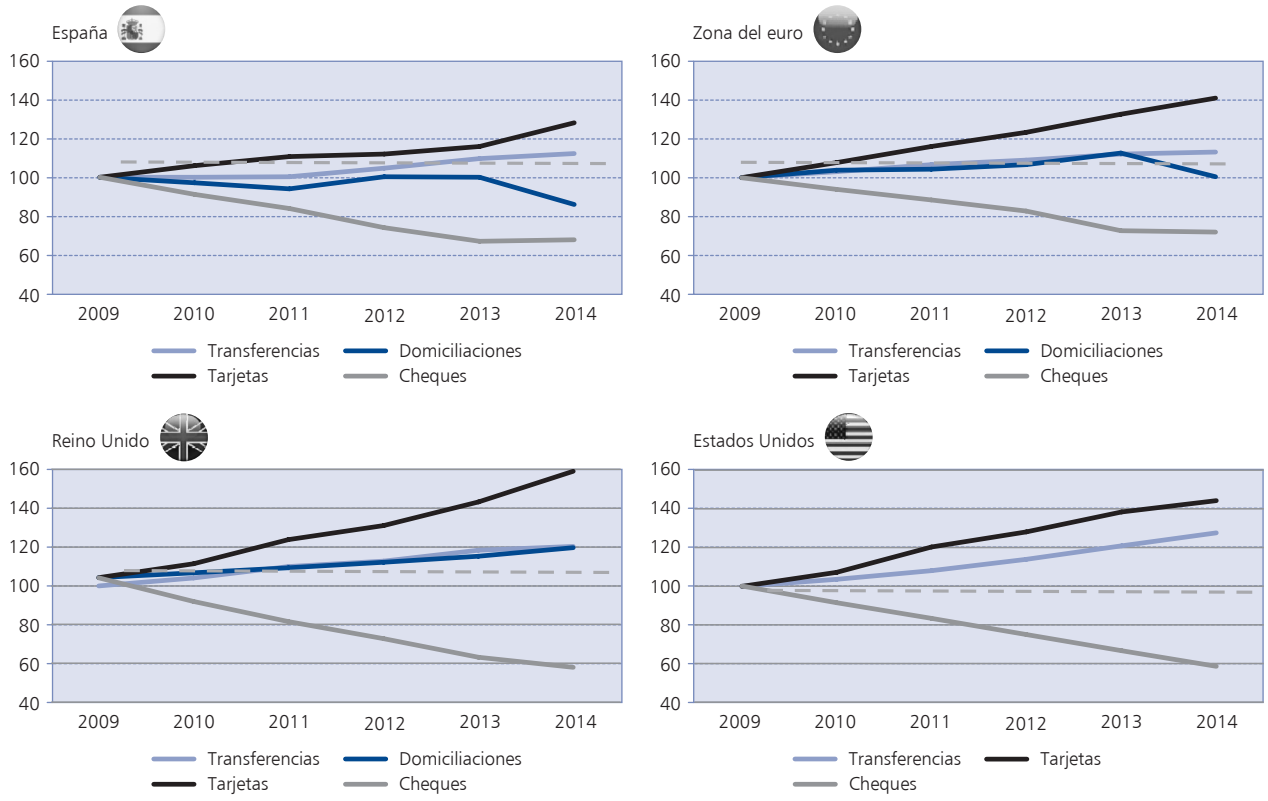
No solo los organismos públicos y los bancos impulsan la utilización de otros medios de pago alternativos, también los propios consumidores están modificando sus hábitos de pago, mostrando su preferencia por instrumentos como las tarjetas de crédito y débito o las transferencias.

Los datos publicados por el Banco de España (BE) y el Banco Internacional de Pagos revelan que entre 2009 y 2014, las transacciones realizadas con instrumentos distintos del efectivo experimentaron un crecimiento en las principales economías desarrolladas. En España, el incremento se situó en el 2,5 por 100, algo menor al 3,4 por 100 de la zona del euro, al 3,9 por 100 de Estados Unidos, y lejos del 6 por 100 del Reino Unido, debido, principalmente, al grave efecto de la crisis económica en nuestro país. Cabe destacar el aumento generalizado en todas las geografías en transacciones de tarjetas, significativamente superior al experimentado por otros instrumentos de pago.

De entre los diferentes instrumentos, las tarjetas son el más utilizado, constituyendo en torno al 50 por 100 de todas las transacciones realizadas y representando, aproximadamente, el 90 por 100 del valor de las mismas.

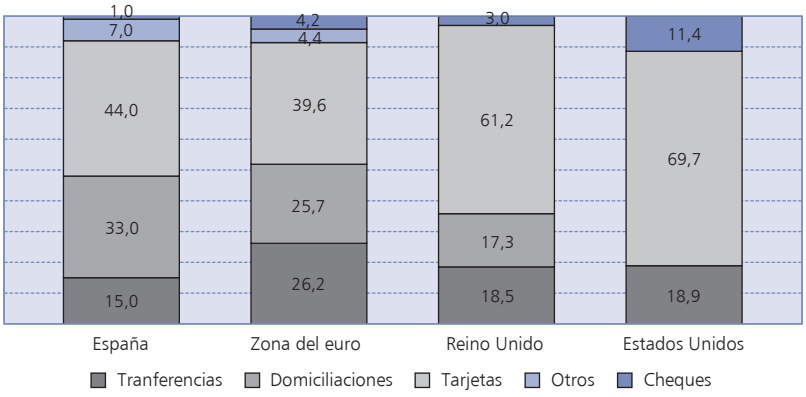
Un estudio realizado por Visa Europe en cinco países europeos a compradores entre 16 y

GRÁFICO 2
CRECIMIENTO INTERNACIONAL DEL VOLUMEN DE PAGOS ELECTRÓNICOS POR TIPO DE INSTRUMENTO (BASE 100 EN 2009; ENTRE 2009 Y 2014)



Fuentes: BIS, BE. Análisis Accenture.

GRÁFICO 3
DISTRIBUCIÓN INTERNACIONAL DE LAS TRANSACCIONES DISTINTAS DEL EFECTIVO POR TIPO DE INSTRUMENTO (% OPERACIONES; 2014)



Fuentes: BIS, BE.

65 años viene a corroborar estas cifras. El 54 por 100 de los consumidores prefieren comprar en establecimientos en los que se acepta la tarjeta como medio de pago por la seguridad y comodidad que les confiere, y este porcentaje llega a alcanzar el 71 por 100 en el caso de compras superiores a 100 £.

2. La importancia del comercio electrónico y móvil

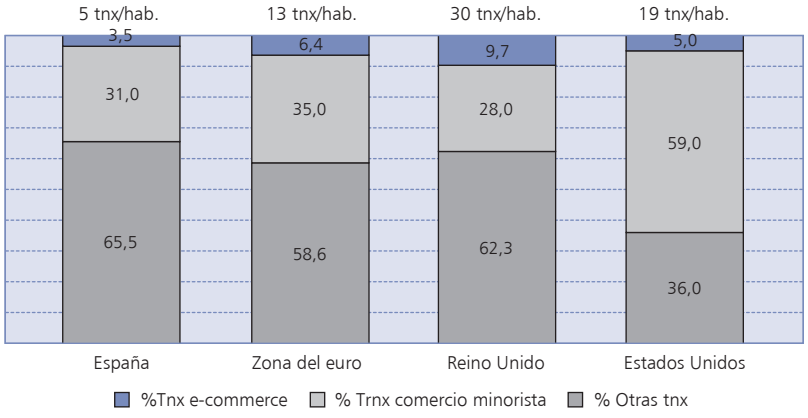
La evolución creciente del comercio, en concreto del comercio electrónico, también está favoreciendo el auge de los medios de pago. La revolución digital en la que nos encontramos inmersos ha propiciado que los particulares y comercios compren y vendan cada vez más a través de la red, generando un espectro de posibilidades mucho mayor que en el comercio físico tradicional.

Las transacciones del comercio electrónico en 2014 representaron en España ~3,5 por 100 del total del comercio (equivalente a 5 transacciones por habitante al año), una relación menor a la de la zona del euro (~6,4 por 100, representando 13 transacciones por habitante al año), Reino Unido (~9,7 por 100, representando 30 transacciones por habitante al año) y Estados Unidos (~5,0 por 100, representando 19 transacciones por habitante al año).

No obstante, si bien España se encuentra en el grupo de países de la Unión Europea (UE) caracterizados por una baja penetración del comercio electrónico, presenta uno de los mayores crecimientos de la zona en los últimos años (~17 por 100), demostrando que los pagos en el comercio electrónico son foco de especial atención por parte de las entidades y de demanda de nuevos servicios de valor por parte de los usuarios.

Dentro del comercio electrónico, los pagos a través del teléfono móvil también cobran protagonismo, llegando a suponer entre el 7 y el 20 por 100 de todas las compras *online* del conjunto de países de la UE. España presentó en 2014 una penetración del 10 por 100, si bien se espera llegue a niveles próximos al 20 por 100 a finales de 2016 debido al incremento en el uso de teléfonos inteligentes en todos los grupos de edad. En nuestro país, la penetración de este tipo de dispositivos (88 por 100) es superior a la media europea.

GRÁFICO 4
DISTRIBUCIÓN INTERNACIONAL DE LAS TRANSACCIONES DE PAGO DE COMERCIO ELECTRÓNICO *VERSUS* TRANSACCIONES DE PAGOS *OFFLINE* (% TRANSACCIONES; 2014)



Fuente: BIS, Accenture.

Estos datos muestran que las soluciones de pago basadas en el móvil serán clave en los próximos años por su ubicuidad e inmediatez, tanto para pagos físicos como para pagos *in-app*.

Es indiscutible que el teléfono facilita la homogeneización de la experiencia en el comercio físico y en el *e-commerce*, lo que puede suponer una ventaja competitiva para las marcas globales frente a los sistemas que operan solo en uno de los mundos. Los usuarios de pagos en ambos entornos buscan, cada vez más, no solamente la sencillez, sino también una experiencia análoga que les permita además disfrutar de servicios de valor añadido tanto pre como pospago.

Por ello, el móvil se presenta hoy en día como el nuevo campo de batalla del mundo de pagos para conseguir usuarios. Como dato relevante, los españoles solo usan ocho aplicaciones de veinte que se descargan, lo que significa que las entidades financieras y proveedores de servicios de pago (PSP) deberán esforzarse en lanzar aplicaciones atractivas para los consumidores, siendo importante facilitar una experiencia integrada, garantizar la seguridad de las transacciones y realizar un esfuerzo comercial para que la marca utilizada sea reconocida en el mercado.

3. La pérdida de la hegemonía de los bancos

Ante el crecimiento exponencial del comercio electrónico y la creciente universalidad del móvil, otros «jugadores» distintos de las entidades financieras han comenzado a interesarse por las soluciones para el *client to retail* («cliente a comercios», C2R). En concreto, la entrada de Apple Pay ha supuesto un fuerte revulsivo mediante una experiencia de usuario sobresaliente.

Google, por su parte, ha evolucionado en una dirección similar con Android Pay, con la diferencia de que es un sistema abierto, por lo que proporciona mayores opciones a la banca, puesto que le permite desarrollar soluciones en colaboración con Android Pay o su propio monedero electrónico o *e-wallet*.

En torno a las transferencias bancarias han surgido también soluciones alternativas, como los OBeP (*online banking e-payments*), soluciones que permiten dar respuesta a las necesidades de los clientes para diferentes casos de uso como el C2R o el C2C (*Client to Client* o «cliente a cliente») y competir directamente con las tarjetas. OBePs como Sofort y Trusly son pagos a través de la banca *online* basados en transferencias con confirmación inmediata de la operación y disposición de fondos diferida.

La segunda Directiva sobre Servicios de Pago o PSD2 introduce nuevos aspectos regulatorios que favorecen la reciente multiplicación de nuevos competidores y soluciones. La norma europea establece que los pagadores puedan hacer uso de «proveedores de iniciación del pago» (o PISP) y de «proveedores de servicios de información de cuenta» (AISP), estando este derecho confinado a las cuentas *online*. Esta implicación supone, entre otros, que los bancos estén obligados a comunicarse de forma segura con los PISP y AISP, a proveerles con toda la información disponible relativa a la ejecución de la transacción, o a tratar las órdenes de pago o de información sin ninguna discriminación.

No obstante, los usuarios siguen mostrando su respaldo a las entidades financieras. Un reciente estudio de Accenture revela que a la hora de hacer uso de un medio de pago, más del 82 por 100 de los encuestados optarían por bancos, frente al 63 por 100 que optarían por las compañías tecnológicas y el 48 por 100 por empresas de telefonía. La regulación a la que están sometidos los bancos y la probada seguridad en sus pagos, demostrada a lo largo de los años, hacen que los particulares sigan confiando en las entidades financieras para realizar los pagos de forma segura.

No obstante, en un entorno de pagos convulso como el actual, las entidades financieras tendrán que decidir su estrategia y determinar por qué soluciones de pagos apostar para proteger su papel como actores relevantes del ecosistema de pagos.

Es en este contexto de eliminación del efectivo, de crecimiento del comercio electrónico y de emergencia de nuevos actores, en los que factores como la seguridad y la identidad digital surgen como pilares necesarios para la creciente y definitiva adopción de los servicios de pago electrónico.

II. LA SEGURIDAD COMO ELEMENTO ESTRATÉGICO DE LOS PAGOS

1. La seguridad en pagos electrónicos

La seguridad en pagos electrónicos se entiende como la protección de la información de las transacciones, garantizando su confidencialidad (únicamente accederá a la misma quien se encuentre autorizado), su integridad (la información será

exacta y completa) y su disponibilidad (los usuarios accederán a la información cuando lo requieran).

La seguridad constituye una de las principales preocupaciones para las entidades financieras puesto que cualquier brecha implica no solo importantes pérdidas económicas sino un daño potencialmente irreversible a la reputación de la compañía. Algunos ejemplos recientes en diferentes industrias ponen de relieve el impacto del fraude: en 2012 Global Payments sufrió un robo de 10 millones de tarjetas de crédito con un coste directo de 100 millones de dólares; en 2012 a Subway le sustrajeron 146.000 tarjetas con un coste directo asociado de 10 millones de dólares; en 2012 StarDust padeció el robo de 20.000 tarjetas; en 2013 Target sufrió un robo de 40 millones de tarjetas y datos de 110 millones de clientes, con un coste directo de 30 millones de dólares; en 2014 Home Depot fue objeto de robo de 56 millones de tarjetas.

2. Magnitud e impacto del fraude

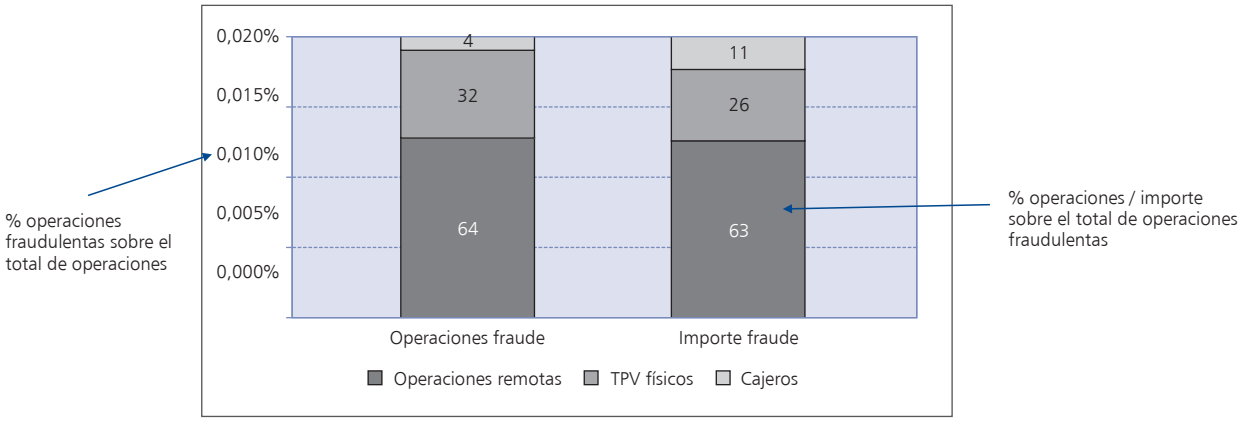
Los últimos datos publicados por el BE en su memoria anual sobre la vigilancia de sistemas de pago muestran que en 2014 se registraron 743.000 operaciones fraudulentas con tarjetas emitidas en nuestro país, por un importe de 46 millones de euros. Estos números suponen unas tasas de fraude del 0,021 por 100 tanto en número de operaciones de venta como en importe, en línea con las tasas del 0,019 por 100 y 0,020 por 100 de los años previos.

Del total de operaciones fraudulentas, un 64 por 100 se correspondió con el fraude en compras realizadas de forma remota, un 32 por 100 a través de TPV físicos y un 4 por 100 en cajeros. En términos de importe, el fraude en compras a distancia supuso un 63 por 100, seguido de los terminales punto de venta, TPV físicos (26 por 100) y de los cajeros automáticos (11 por 100).

En cuanto a la procedencia, el mayor número de operaciones fraudulentas corresponde a las operaciones realizadas en el extranjero con tarjetas emitidas en España, siendo el volumen medio de este fraude un 0,23 por 100 del total de operaciones realizadas en el extranjero. Le siguen las operaciones ejecutadas en nuestro país con tarjetas emitidas en el extranjero (0,10 por 100) y las operaciones realizadas en España con tarjetas nacionales (0,01 por 100). En cajeros, el mayor volumen de fraude se sitúa en las operaciones realizadas en el extranjero con tarjetas emitidas en España, con un 0,16 por 100 del total de los reintegros realizados en el extranjero.

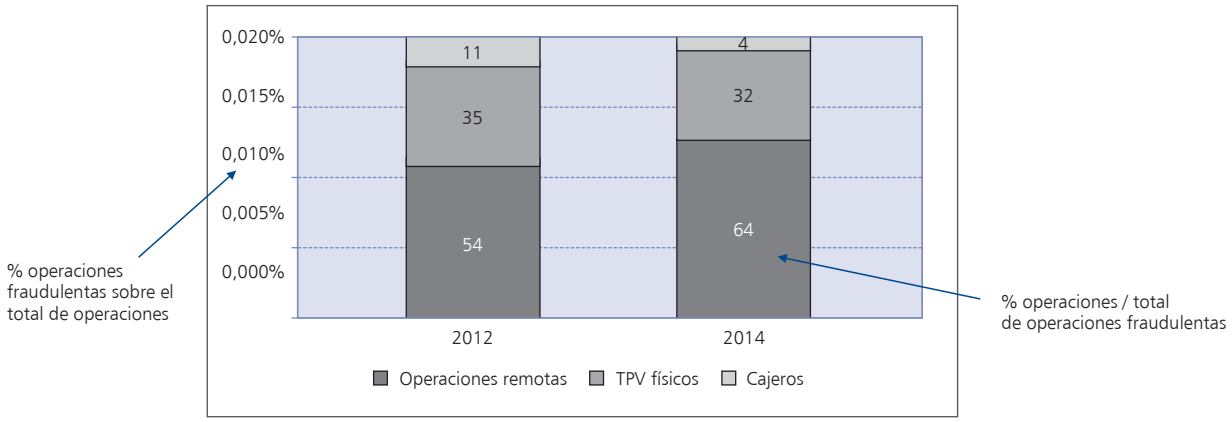
Sin duda, la contención en el crecimiento del fraude asociado a canales más tradicionales como TPV y cajeros se debe a la madurez que los bancos y procesadores han adquirido en la gestión del fraude y la evolución de las herramientas y sistemas de detección de los mismos.

GRÁFICO 5
DISTRIBUCIÓN DE LAS OPERACIONES E IMPORTE DE FRAUDE EN TARJETAS POR CANAL EN ESPAÑA (% OPERACIONES/IMPORTE DE FRAUDE POR CANAL; 2014)



Fuente: Memoria Anual sobre la Vigilancia de los Sistemas de Pago 2014, Banco de España.

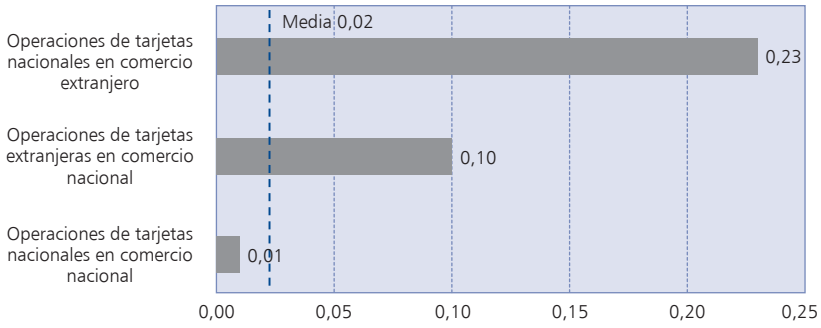
GRÁFICO 6
EVOLUCIÓN DE LAS OPERACIONES DE FRAUDE EN TARJETAS POR CANAL EN ESPAÑA (% OPERACIONES DE FRAUDE POR CANAL; COMPARATIVA 2012 - 2014)



Fuente: Memoria Anual sobre la Vigilancia de los Sistemas de Pago 2014, Banco de España.

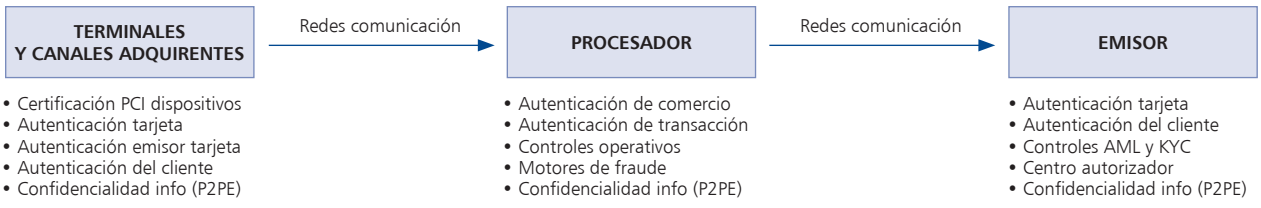
Los mecanismos actuales de análisis de las características de las operaciones de pago para detectar patrones de comportamiento fraudulento e identificar puntos de entrada sospechosos, combinado con sistemas de alertas, está ampliamente implantado en el sector. Adicionalmente, estándares como el EMV (de las siglas de las empresas que lo lanzaron: Europay, Mastercard y Visa) también han favorecido la reducción drástica del fraude en los pagos físicos debido a la sustitución de la tradicional banda magnética de las tarjetas por un chip, evitando el fraude asociado a la lectura de banda.

GRÁFICO 7
DISTRIBUCIÓN DE OPERACIONES DE FRAUDE EN TARJETAS NACIONALES E INTERNACIONALES (% DE OPERACIONES; 2014)



Fuente: Memoria Anual sobre la Vigilancia de los Sistemas de Pago 2014, Banco de España.

GRÁFICO 8
ESQUEMA DE CONTROLES DE SEGURIDAD EN TARJETAS BANCARIAS



Fuente: Experiencia Accenture.

El robo o la pérdida también ha sido una de las principales amenazas de los pagos con tarjeta, pero sin duda la suplantación de identidad y el uso fraudulento del número de tarjeta son las estafas más comunes hoy en día asociadas a los pagos presenciales, pero también virtuales. Como comentábamos con anterioridad, la incorporación del estándar EMV a la industria financiera, a pesar de no estar totalmente extendido en todas las geografías, ha visto decrecer de forma importante otro de los principales focos de fraude basado en la clonación o skimming de tarjetas.

La irrupción de medios de pago basados en el móvil y en Internet plantea nuevos retos en lo que a la seguridad se refiere (tasa de fraude del 0,2 por 100 en operaciones remotas *versus* tasa 0,01 por 100 presenciales). Por ello, la gestión de las nuevas amenazas resulta vital para el desarrollo de los pagos. Si las entidades financieras, procesadores y proveedores de servicios de pago no la garantizan en el nuevo entorno virtual, los usuarios no se mostrarán receptivos a utilizar nuevas soluciones.

En un reciente estudio realizado por Accenture se pone de manifiesto que el 50 por 100 de los usuarios españoles considera que la principal causa para la no utilización del móvil como canal de realización de pagos es la falta de seguridad y fiabilidad. Los *millenials* están impulsando la adopción de aplicaciones móviles, pero sus puntos de vista sobre la importancia de la seguridad en las aplicaciones está tan arraigada como en otros grupos de edad.

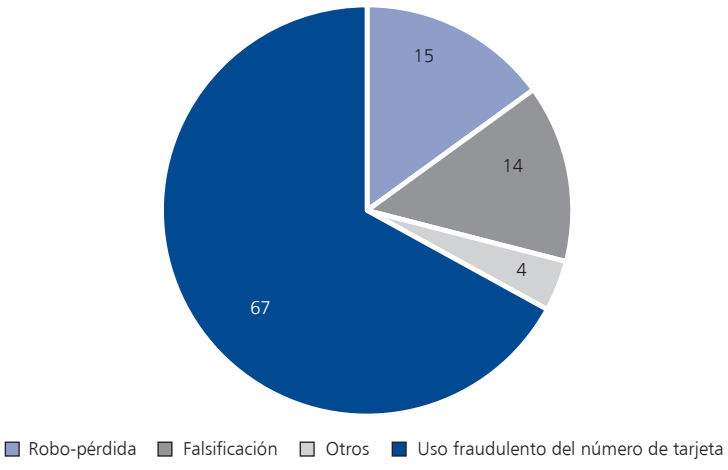
3. Ciberseguridad: amenazas en el espacio digital

La creciente proliferación de soluciones móviles y del uso de Internet hace que cuando se habla de la seguridad en los pagos para los próximos años se piensa en gran medida en la ciberseguridad. La protección de los pagos no se centra únicamente en la propia transacción, sino también en el canal por el que se lleva a cabo. ¿Pero cuáles son las amenazas reales a las que los diferentes intervinientes del ecosistema de pagos se enfrentan? Principalmente, las siguientes:

1. *Phishing:* el ciberdelincuente se hace pasar por otra persona o empresa a través de un correo electrónico en el que solicita el usuario y contraseña para algún tipo de servicio, empleándolos posteriormente con fines fraudulentos. El sector bancario es el segundo más afectado por este tipo de amenazas, seguido de cerca por el sector de los pagos. Como muestran las cifras de Kaspersky, las empresas más afectadas en 2014 por el *phishing* dentro del sistema de pagos fueron Amazon, Apple y e-Bay.

2. *DDO:* del inglés *Distributed Denial of Service*; es una pérdida de conectividad de la red por una saturación de ancho de banda. Se suele llevar a cabo a través de *botnets* (donde el artífice puede controlar diferentes ordenadores / servidores infectados de manera remota), una de las técnicas de ciberataque más usual debido a su sencillez tecnológica y su eficacia. Un ejemplo fue la banca electrónica del HSBC (Hong Kong and Shanghai Banking Corporation, por sus siglas en inglés), víctima de un DDO en enero de 2016. Su red fue colapsada, impidiendo a los clientes realizar ningún tipo de operación. Este tipo de ataques repercuten negativamente en los usuarios, que ven la seguridad de sus finanzas seriamente amenazada, además de suponer un serio riesgo reputacional. Asimismo, constituyen un importante riesgo para el comercio electrónico.

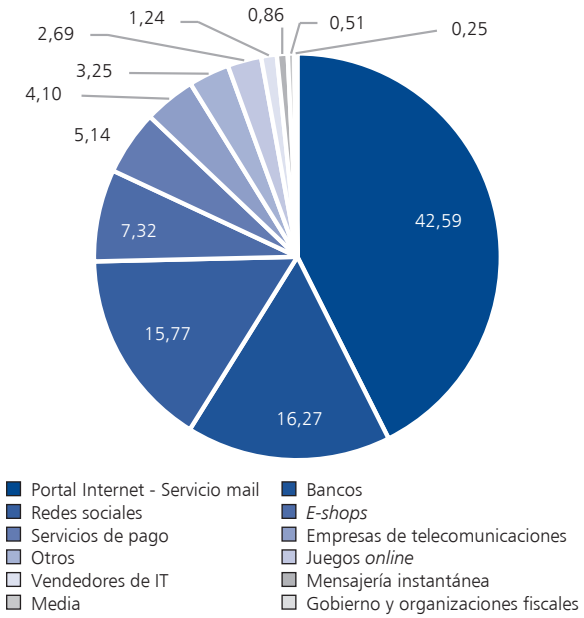
GRÁFICO 9
DISTRIBUCIÓN DE LAS OPERACIONES DE FRAUDE EN TARJETAS POR ORIGEN (% DE OPERACIONES; 2014)



Fuente: Memoria Anual sobre la Vigilancia de los Sistemas de Pago 2014, Banco de España.

GRÁFICO 10

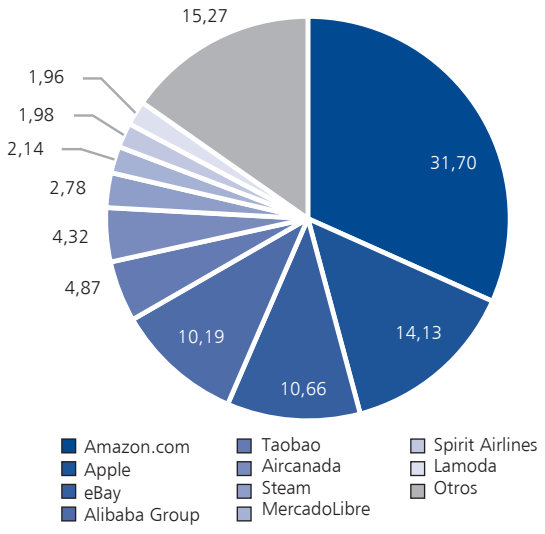
DISTRIBUCIÓN DE CASOS POR SECTOR EN LOS QUE LAS TECNOLOGÍAS *ANTIPHISHING* SE ACTIVARON EN LOS LABORATORIOS KASPERSKY (% DE CASOS; 2014)



Fuentes: Financial Cyberthreats in 2014, Kaspersky Lab Report (2015).

GRÁFICO 11

DISTRIBUCIÓN DE CASOS EN EL SECTOR DE PAGOS EN LOS QUE LAS TECNOLOGÍAS ANTIPHISHING SE ACTIVARON EN LOS LABORATORIOS KASPERSKY (% DE CASOS; 2014)



Fuentes: Financial Cyberthreats in 2014, Kaspersky Lab Report (2015).

3. *Malware: Malicious software* (*software* malicioso) es un tipo de *software* que tiene como fin dañar un sistema sin el consentimiento del propietario. Con la proliferación de la banca por Internet y la banca móvil, este tipo de ataques ha crecido de forma exponencial en los últimos años. Dado que las entidades financieras utilizan con frecuencia el número de teléfono móvil para la autorización de determinados pagos, estos dispositivos se han convertido en un claro objetivo para los delincuentes cibernéticos para ejecutar pagos y transferencias desde la cuenta bancaria de los usuarios. Los troyanos bancarios son las amenazas móviles más extendidas, constituyendo actualmente más del 95 por 100 del *malware* móvil. En concreto, más del 98 por 100 de estos ataques de banca móvil son en dispositivos Android, por dos motivos: el primero es que es la plataforma más popular en el mundo, representando más del 80 por 100 del mercado mundial de teléfonos inteligentes, y la segunda es que el sistema operativo de Android es abierto, por lo que las aplicaciones se pueden descargar en diferentes tiendas que no pasan ningún tipo de control de seguridad (contrariamente a lo que sucede con Apple y su AppleStore).

Pero también los cajeros automáticos están siendo víctima de ataques de *malware*. En 2015, aproximadamente 100 entidades bancarias se habían visto afectadas por un *malware*, la mitad de ellas con importantes pérdidas financieras.

4. *Keylogger:* otro *malware* consistente en registrar las pulsaciones que se hacen en el teclado del ordenador o en la pantalla táctil del teléfono. De esta forma, el *software* es capaz de registrar números, usuarios y contraseñas

asociadas a diferentes instrumentos de pago.

5. *Ransomware:* el *software* de rescate o *ransom software* es un tipo específico de *malware* consistente en restringir el acceso al usuario a determinadas partes o archivos de su sistema, solicitando una recompensa monetaria a cambio del restablecimiento del servicio. Comenzó a expandirse en Rusia en 2013, y desde entonces su crecimiento ha sido imparable. En 2014 se detectaron 7 millones de intentos de infección por *ransomware*, experimentando un crecimiento del 65 por 100 entre finales de 2014 y el primer trimestre de 2015. El robo de información de tarjetas de crédito y la transferencia de dinero desde el teléfono móvil son dos ejemplos de lo que pueden hacer los troyanos bancarios, como el *ransomware*, en un dispositivo móvil.

4. Cómo minimizar los riesgos

Los riesgos en el mundo virtual de los pagos son crecientes. Para hacerles frente es necesario actuar en cuatro frentes:

— La regulación y estándares.

— La educación de los usuarios.

— La tecnología.

— El papel de las entidades financieras.

4.1. Regulación y estándares

La supervisión y regulación por parte de organismos nacionales e internacionales es el primer pilar sobre el que recae la lucha contra el fraude y el cibercrimen.

En relación a las tarjetas físicas, existen dos importantes estándares que han propiciado el descenso en los últimos años del fraude asociado a este instrumento. Por una parte, el PCI DSS (*Payment Card Industry Data Security Standard* o Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta) que incluye doce requisitos operacionales y técnicos definidos por el Consejo de Estándares de Seguridad de la Industria de Pagos con Tarjeta creado en 2006 por las principales marcas (American Express, Visa, Mastercard, Discover y JCB). La norma PCI DSS está enfocada a los diferentes actores dentro del mundo de pagos (entidades financieras, procesadores, comercios físicos y electrónicos, etc.) de cara a proteger los datos del titular de la tarjeta y de autenticación dentro del ecosistema de pagos, limitando su disponibilidad para los estafadores e implicando importantes sanciones económicas para aquellos responsables que no la cumplan.

GRÁFICO 12

TABLA RESUMEN DE LOS PRINCIPALES RIESGOS ASOCIADOS A LOS MEDIOS DE PAGO

DOMINO	*RIESGO*	*CAUSAS MÁS COMUNES*
Identificación del pagador	• Uso fraudulento de medios de pago: - Robo - Clonación - Suplantación de identidad • Lavado de dinero	Falta de seguridad en la identificación del pagador
Identificación del receptor (comerciantes y mediadores)	• Comercios fraudulentos • Suplantación de identidad del comercio o mediador (*Phising*)	Falta se seguridad en la identificación del receptor
Canal seguro	• Fuga de datos en tránsito • Pérdida de integridad de transacciones	Ataques al canal de transmisión tanto entre el pagador y el comercio/mediador como en el *back-end* (entre el mediador y el comercio)
Almacenamiento seguro	• Fuga de datos • Pérdida de integridad de transacciones • Falta de disponibilidad de procesos/ plataformas	• Errores de diseño/codificación • Infraestructuras inseguras • *Malware*
Proceso seguro	• Fuga de datos • Pérdida de integridad de transacciones • Falta de disponibilidad de procesos/ plataformas	• Errores de diseño/codificación • Infraestructuras inseguras • *Malware* • Procesos de negocio mal diseñados

Fuente: Accenture.

Por otra parte, el estándar EMV, comentado anteriormente, ha supuesto un refuerzo a la seguridad en los pagos con tarjeta, utilizando algoritmos de cifrado para la provisión de autentificación de la tarjeta al terminal que la procesa, y a la entidad que realiza la transacción. La prueba de la eficacia de este sistema es que del total de fraudes detectados en nuestro país, la mayoría provienen de tarjetas de origen español que han realizado alguna compra en un punto de venta de países en los que todavía no se ha adoptado el EMV, como Estados Unidos o algunos países latinoamericanos.

En el ámbito europeo, y relacionado con los pagos virtuales, el Banco Central Europeo (BCE) publicó en noviembre de 2013 un documento en el que recopilaba una serie de recomendaciones para la seguridad de los pagos por internet aplicables a los PSP, así como a las autoridades responsables del gobierno de los esquemas de pago. Estas encomiendas, elaboradas por el Foro Europeo de Pagos Minoristas (SecuRe Pay), se pueden resumir, tal y como indica el BE, en los siguientes puntos:

1. *Proteger la realización de pagos a través de Internet*, así como el acceso a datos confidenciales de pagos, a través de un riguroso procedimiento de autenticación de clientes.

2. *Limitar el número de intentos de conexión* o de autenticación, definir las normas aplicables al «tiempo de espera» en las sesiones, al utilizar servicios de pago por Internet, y fijar plazos de validez de la autenticación.

3. *Establecer mecanismos de seguimiento* de las operaciones diseñados para prevenir, detectar y bloquear operaciones de pago fraudulentas.

4. *Introducir varios niveles de seguridad* para reducir los riesgos identificados.

5. *Facilitar asistencia y orientación a los clientes* acerca de buenas prácticas de seguridad en Internet, crear alertas y proporcionar herramientas para ayudar a los clientes a realizar un seguimiento de las operaciones.

Por otra parte, el organismo europeo también sacó a la luz un listado de recomendaciones específicas para los pagos móviles dirigidas a los MPSP *(Mobile Payment Service Providers o* Proveedores de Servicios de Pago Móvil*)*. Algunas de estas iniciativas están incorporadas en la PSD2 y se basan en cinco pilares básicos:

1. *Identificar, evaluar y mitigar* los riesgos específicos asociados a los servicios de pago, teniendo en cuenta los riesgos que puedan resultar de la dependencia de terceros, tales como operadores de redes móviles, TSMs *(Trusted Service Providers o Proveedor de Servicios de Confianza)*, así como fabricantes de elementos seguros y otros componentes.

2. *Proteger* la iniciación de los pagos móviles y el acceso a los datos sensibles de pago a través de una autenticación fuerte de los usuarios. Se considera que una autenticación es fuerte cuando se utilizan dos o más de los siguientes elementos: i) algo que solo conoce el usuario (p.ej.: una clave, un código, un número de identificación, etc.); ii) algo que sólo posee el usuario (p.ej.: un *token*, una tarjeta electrónica, un dispositivo móvil, etc.); iii) algo que el usuario es (p.ej.: característica biométrica).

3. *Implantar mecanismos sólidos de protección* de la información sensible transmitida, procesada y/o almacenada.

4. *Implantar métodos seguros* para autorizar las transacciones y monitorizarlas de cara a la prevención del fraude.

5. *Fomentar la sensibilidad y educación* de los usuarios en materia de seguridad.

Todas estas recomendaciones constituyen una forma de regular los mínimos de seguridad a llevar a cabo para disminuir los riesgos de fraude y robo de información a la hora de realizar los pagos, y el establecimiento de un estándar común en los diferentes países europeos.

4.2. Educación de los usuarios

Como señala el Banco Central Europeo, la formación de los usuarios en términos de seguridad es uno de los elementos primordiales para garantizar los pagos. Con frecuencia, se asocia la falta de seguridad con ataques provenientes de *hackers* o ciberdelincuentes, pero lo cierto es que el primer paso para que los pagos se realicen de forma segura es la correcta utilización que los propios particulares hacen de la información sensible y de sus teléfonos móviles. La causa más evidente es el uso o almacenamiento no adecuado de contraseñas o la pérdida del propio dispositivo, que pueden conllevar el robo de información relevante sobre el usuario.

Otra de las causas es comprometer la seguridad de los dispositivos. Por ejemplo, el de-

nominado *jailbreak*. Esta práctica solo es aplicable al sistema operativo de Apple y consiste en que el usuario suprima alguna de las limitaciones incorporadas en el sistema operativo iOS, permitiéndole descargar aplicaciones no disponibles en el AppleStore y que pueden incorporar algún tipo de *malware*. En general, y para cualquier sistema operativo, es importante que los individuos se conciencien de que los teléfonos inteligentes y las tabletas están sometidos a las mismas amenazas que los ordenadores de sobremesa o portátiles, por lo que la instalación de *software* de seguridad es un elemento fundamental en la protección.

Por último, el uso de contraseñas débiles, o la no utilización del doble factor de autenticación introducido por el BCE, pueden constituir otra de las causas más frecuentes de quiebre de la seguridad.

Por parte de los comercios, también resulta imprescindible que aquellos que venden a través de Internet protejan adecuadamente su sitio web y el almacenamiento de datos, ya que suponen hoy en día un blanco fácil para los ciberdelincuentes.

En este sentido, los diferentes intervinientes del mundo de pagos, pero en especial las entidades financieras, juegan un papel importante en la educación y concienciación de los clientes en el buen uso del dispositivo móvil.

4.3. Tecnología

En los pagos móviles, la tecnología asociada a la seguridad se centra en el propio teléfono, en concreto al almacenaje y protección de la información de la tarjeta de crédito o cuenta bancaria. Existen diferentes modalidades:

1. *Tarjeta SIM:* la GSMA (Global System for Mobile Communications Association o Asociación de Sistemas Globales para las Comunicaciones Móviles), Visa y Mastercard y los fabricantes de dispositivos respaldaron en un inicio las soluciones móviles de pago en tienda basadas en SIM (Subscriber Identity Module o Módulo de Identidad del Suscriptor). No obstante, está comprobado que esta tecnología está destinada a la obsolescencia, debido principalmente a la baja experiencia de usuario, una propuesta de valor poco clara para el emisor por el coste que implica y la falta de propuesta de valor al usuario.

2. *HCE:* el almacenamiento en la SIM está siendo remplazada por el nuevo estándar HCE (*Host Card Emulation* o Host de Emulación de Tarjeta) que tiene el potencial de simplificar significativamente los modelos de negocio de los pagos móviles y cuya información se guarda en la nube. Se trata de una nueva arquitectura de *software* implementada en Android e introducida en noviembre de 2013 que permite a cualquier aplicación imitar una tarjeta inteligente NFC (Near Field Communication, por sus siglas en inglés) y hablar directamente al lector. Presenta, además, una clara ventaja para las entidades financieras, ya que a la hora de lanzar sus soluciones de pagos móviles, estos pueden tomar el control de su propia información y del entorno de pagos, al ser un sistema abierto. En España, los principales bancos ya están empleando esta tecnología. Los elementos de seguridad de la transacción quedan alojados en los sistemas del banco en lugar de en el *hardware* del dispositivo.

3. *SE:* del inglés Secure Element o elemento seguro, es un chip que permite guardar de forma segura y encriptada el código y la información financiera de los usuarios en los sistemas de pagos móviles. El caso más conocido en el mercado de utilización del SE es Apple. Según la compañía norteamericana, si alguien intentase *hackear* el sistema operativo de uno de sus teléfonos, no podría extraer la información financiera porque esta nunca se guarda en el *software* del dispositivo, sino en un componente físico del mismo o *hardware*.

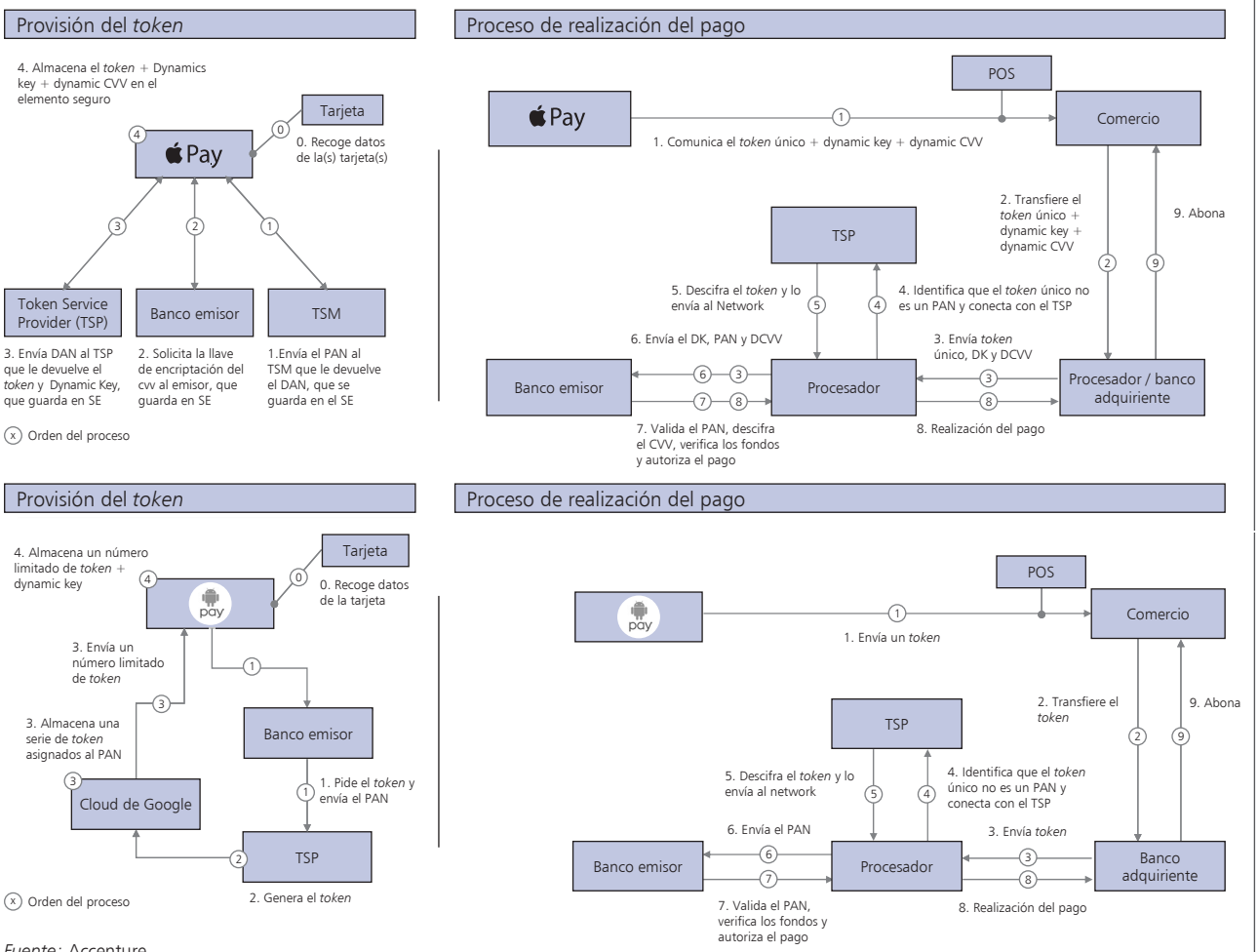
Tanto para las soluciones HCE (con almacenamiento de la información en la nube) o las soluciones SE (con almacenamiento de la información en el *hardware*), hay un componente adicional que incrementa la seguridad de los pagos: la *tokenización*. Permite aumentar la seguridad de las transacciones al sustituir los datos de pago, como la cuenta bancaria o la tarjeta, por un *token* o número aleatorio único para cada transacción. Facilita la realización de operaciones sin que los datos bancarios pasen por los sistemas del comercio. Los datos permanecen en el banco emisor y en el proveedor de servicios de *tokenización*.

4.4. Papel de las entidades financieras

Si bien gran parte de las medidas encaminadas a proteger los pagos y minimizar la posibilidad de ciberataques provienen directamente del comportamiento del usuario y de la tecnología asociada a los dispositivos móviles, las entidades financieras, por su parte, tienen un papel relevante.

El gran reto de la banca es equilibrar sus niveles de segu-

GRÁFICO 13
ESQUEMAS DE *TOKENIZACIÓN* DE APPLE Y ANDROID



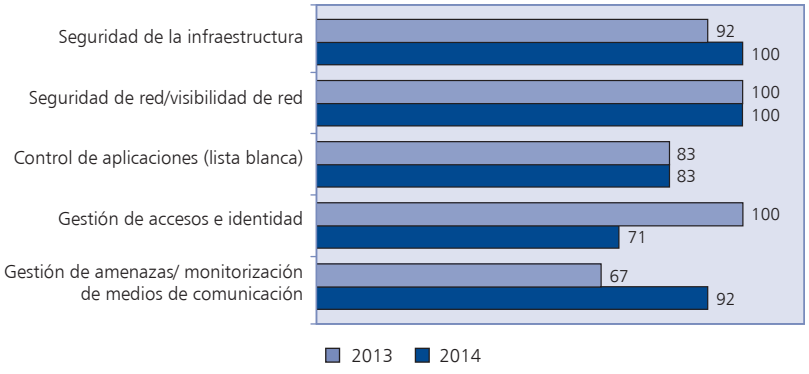
Fuente: Accenture.

ridad con la usabilidad. Es cierto que la seguridad es un valor esencial, pero no a costa de comprometer la adopción de uso del servicio, pues podemos llegar a la paradoja de que el servicio de pago más seguro es el que no se utiliza. Por ello, es necesario alcanzar un correcto balance entre la experiencia de usuario (UX), cada vez más tendente a la simplicidad y homogenización entre los diferentes casos de uso de pago, y la seguridad.

El *Estudio de Costes de Tecnologías de la Información en las Entidades Financieras* de 2014 elaborado por Accenture pone de manifiesto la creciente preocupación de los bancos españoles por reforzar los mecanismos de prevención, detección y respuesta ante ataques informáticos. El sector financiero es consciente de la importancia de la seguridad en el nuevo ecosistema digital y se robustece potenciando las tecnologías de seguridad. En 2014, se constató un crecimiento en la implantación de tecnologías de detección y de respuesta a amenazas a través del análisis de inteligencia de fuentes externas como complemento a los sistemas de seguridad tradicionales.

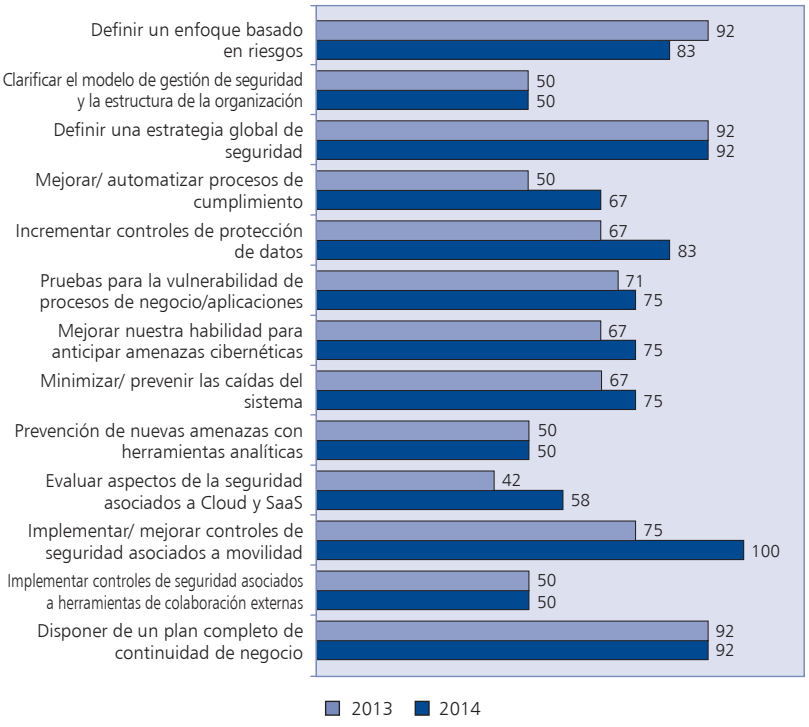
Por otra parte, se observó que la mayoría de las entidades otorgan una prioridad alta o muy alta a las funciones de seguridad, aunque a medida que se implantan nuevas tecnologías estas requieren de una revisión constante para gestionar la aparición de nuevas amenazas. Entre las prioridades de seguridad de las entidades financieras españolas, respecto a 2013, se intensificaron las relacionadas con la

GRÁFICO 14
COMPARATIVA 2013-2014 DEL PORCENTAJE DE ENTIDADES FINANCIERAS ESPAÑOLAS EN PILOTO O IMPLANTACIÓN DE TECNOLOGÍA DE SEGURIDAD (% DE ENTIDADES; 2013-2014)



Fuente: Estudio de Costes de Tecnologías de la Información en las Entidades Financieras en 2014, Accenture (2015).

GRÁFICO 15
COMPARATIVA 2013-2014 DEL PORCENTAJE DE ENTIDADES FINANCIERAS ESPAÑOLAS CON PRIORIDAD ALTA O MUY ALTA EN LAS FUNCIONES DE SEGURIDAD (% DE ENTIDADES; 2013-2014)



Fuente: Estudio de Costes de Tecnologías de la Información en las Entidades Financieras en 2014, Accenture (2015).

automatización de procesos, la protección de los datos, la gestión de amenazas cibernéticas y el control asociado a Cloud, SaaS y la movilidad.

En cuanto al presupuesto, algunos informes muestran que en 2014 la seguridad representó un 3,8 por 100 del presupuesto total de TI de las entidades, aumentando respecto al 3,5 por 100 de 2012.

5. El futuro de la seguridad asociada a los pagos

Las tendencias en los pagos muestran dos grandes tendencias en la lucha contra el fraude. Por una parte, los modelos paramétricos neuronales de identificación de transacciones fraudulentas evolucionarán hacia modelos no solo de detección del fraude más sofisticados (ex post) sino también hacia modelos predictivos (ex ante), que permitan anticiparse al delito antes de que se produzca. La utilización de tecnologías Big Data y Analytics jugará un papel esencial, facilitando a las entidades financieras y procesadores el desarrollo de modelos individualizados del comportamiento de cada cliente.

Por otra parte, la virtualización de los pagos y el uso exponencial de los móviles va a hacer que una parte importante de la prevención de ataques se centre en la ciberseguridad. Las principales amenazas no se van a circunscribir únicamente al robo de las tarjetas o la copia del número del plástico, sino también a la introducción de virus y ciberataques. Por ello, el desarrollo de arquitecturas, aplicaciones de pago robustas y el refuerzo de los métodos de autenticación van ser

los pilares fundamentales sobre los que trabajar.

III. LA IDENTIDAD DIGITAL

1. Qué es la identidad digital bancaria

A la hora de iniciar un pago a través de cualquiera de las soluciones disponibles en el mercado, cobra especial importancia el concepto de identidad digital. ¿Pero qué es realmente? De forma generalizada, este término se utiliza para referirse a todo lo que se manifiesta en el ciberespacio sobre un individuo u organización. Todas las actuaciones dentro del entorno digital (imágenes, comentarios, *links* visitados, etc.) conforman la denominada identidad o perfil digital.

Dentro del mundo de pagos, la identidad digital no es más que la forma que tenemos de identificarnos, autenticarnos y autorizar los pagos que vamos a realizar.

Incluimos dentro del concepto de identificación digital bancaria los sencillos alias que nos asocian ante terceros con nuestros complejos números de cuenta bancaria (IBAN) o de tarjeta. En este sentido, cabe destacar las múltiples iniciativas existentes en el ámbito internacional que vinculan números de teléfono móvil, direcciones de correo electrónico y/o identificadores de redes sociales, ya registrados en las agendas de nuestros contactos, con números de cuentas o tarjetas bancarias.

2. Usuario y contraseña como método identificativo

La forma más extendida hoy en día es la introducción de un usuario y una contraseña. Muchas de las soluciones que han salido recientemente al mercado utilizan este método, replicando lo que ya se venía empleando en la banca *online* tradicional.

Según un estudio de Accenture, el 60 por 100 de los usuarios considera que la utilización de usuario y clave es un método incómodo de identificación (fragmentación de relaciones con múltiples usuarios diferentes y contraseñas ¿diferentes?). Investigaciones recientes demuestran que casi el 84 por 100 de los consumidores olvida su contraseña en algún momento y se pierden un mínimo de diez/quince minutos cada vez que se olvidan de ella. La dificultad de recordar un número elevado de contraseñas conduce con frecuencia al abandono de compras *online* o al uso de contraseñas débiles, lo que facilita la suplantación de la identidad digital y, por tanto, el incremento de acciones fraudulentas.

En algunos países, se ha dado un paso en la simplificación de la experiencia de usuario para la identificación electrónica a través del denominado BankID (equivalente a nuestro DNI). Es una modalidad de identificación cooperativa de un conjunto de entidades financieras, organismos públicos, autoridades y empresas. Un caso de éxito es el BankID de Suecia, desarrollado por un grupo de bancos, con 6,5 millones de usuarios activos (70 por 100 población), empleado asiduamente en muchos servicios básicos (desde el comercio electrónico, la banca móvil, servicios de pago, hasta la declaración de impuestos) para la identificación digital y la firma de transacciones y documentos.

El 77 por 100 de los usuarios, según cifras de Accenture, muestra su interés en emplear métodos simples alternativos con el fin de proteger su seguridad en Internet.

Por este motivo, se está dando un paso más en la identidad digital mediante la incorporación de aspectos biométricos.

3. Un paso más: los métodos biométricos

La biometría implica utilizar elementos físicos o comportamentales medibles para establecer un patrón que permite identificar y/o verificar la identidad de una persona.

Estos métodos de reconocimiento se emplean en distintos ámbitos, desde el sector público hasta el financiero.

En la India, Accenture llevó a cabo el proyecto denominado «Programa de ID único» en el que se utilizó la biometría para identificar y proporcionar a los ciudadanos un número de identidad único, permitiéndoles acceder a una serie de servicios públicos de forma rápida y sencilla, y en concreto, a un importante segmento de la sociedad que históricamente había sido excluido.

Amazon, por su parte, está desarrollando un sistema que permitirá a los clientes pagar a través de un sistema de reconocimiento facial. Una vez que los clientes hayan seleccionado su compra, la idea es que puedan identificarse mediante un *selfie* y que confirmen el pago con un gesto facial. Como explica Amazon, «las contraseñas pueden ser robadas o descubiertas por alguien que puede suplan-

tarnos la identidad para realizar transacciones».

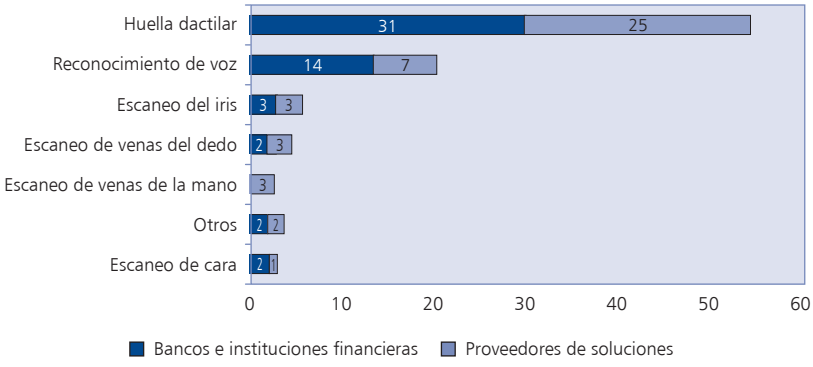
En relación a la industria financiera, bancos de países como Brasil, India, Polonia o Japón ya disponen de cajeros automáticos biométricos que permiten a los clientes retirar dinero o realizar otras transacciones identificándose a través de la lectura de la huella digital o el escáner de las venas dactilares. En Japón, concretamente, hay actualmente más de 80.000 ATM (automated teller machines o cajeros) de este tipo habilitados y más de 15 millones de clientes que los utilizan.

Existen otros ejemplos más próximos como el de Barclays, que introdujo en 2014 el reconocimiento de voz para los clientes de Wealth Management en sus centros de llamadas (*call centers*), y la lectura de las venas de los dedos como método de autenticación para su segmento de Banca Corporativa. En lugar de tener que utilizar contraseñas y claves, los clientes pueden iniciar la sesión en sus cuentas mediante la colocación de uno de sus dedos en un escáner portátil conectado al puerto USB del ordenador. Este dispositivo utiliza infrarrojos para comprobar el patrón único de venas en el interior del dedo, facilitando la experiencia de usuario.

Pero en relación a los pagos, sin duda, el caso que mayor repercusión ha tenido en el último año es el ID Touch de Apple. En 2014, la compañía lanzó en Estados Unidos su sistema ApplePay, mediante el cual se puede pagar a través de un sistema *contactless* (sin contacto) simplemente acercando el teléfono al terminal punto de venta del comercio en el momento de la compra, y autenticándose mediante la lectura de la huella digital. Los sistemas de pago *contactless* tienen la ventaja de la usabilidad, pero incrementan la posibilidad de sufrir robos si se hace un uso fraudulento de los TPV.

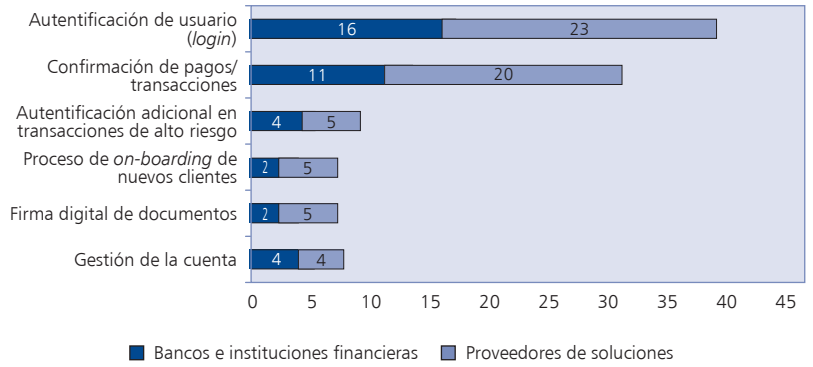
Respecto a las tipologías de reconocimiento biométrico, existe una amplia gama. Las principales se centran la lectura de la huella dactilar, el reconocimiento de voz, el escáner de retina, el escáner de las venas de la mano o de los dedos y el reconcomiendo facial. Una encuesta realizada en 2015 por Mobey Forum a 235 entidades financieras y proveedores de soluciones muestra que los métodos biométricos preferidos por los bancos son la huella digital (31 por 100) y el reconocimiento de voz (14 por 100), y los casos de

GRÁFICO 16
DISTRIBUCIÓN DE LA VOLUNTAD DE UTILIZACIÓN DE MÉTODOS BIOMÉTRICOS POR TIPOLOGÍA, POR PARTE DE ENTIDADES FINANCIERAS Y PROVEEDORES DE SOLUCIONES (% DE ENTIDADES; 2015)



Fuente: Biometrics in payments: Touching convenience, Mobey Forum (2015).

GRÁFICO 17
DISTRIBUCIÓN DE LOS CASOS DE USO MÁS RELEVANTES A LA HORA DE UTILIZAR MÉTODOS BIOMÉTRICOS POR PARTE DE ENTIDADES FINANCIERAS Y PROVEEDORES DE SOLUCIONES (% DE ENTIDADES; 2015)



Fuente: Biometrics in payments: Touching convenience, Mobey Forum (2015).

uso más relevantes a la hora de utilizarlos son la autenticación de los usuarios y la confirmación del pago o transacción.

Accenture ha desarrollado un sistema experto de reconocimiento de patrones biométricos (imagen de la cara, huella digital, escáner de iris y de voz), contra una serie de muestras almacenadas, datos biográficos y contextuales, permitiendo confirmar rápidamente la identidad de un individuo de forma segura y conveniente. Soluciones de aplicación para múltiples áreas incluyendo la policía, la salud, los servicios públicos, los servicios financieros y la educación.

4. El futuro de la identidad digital

El reporte anual de 2015 llevado a cabo por el Instituto de Biometría puso de manifiesto que la industria de servicios financieros será el sector con mayores implantaciones biométricas en los próximos años. Esta tendencia, como indica Mobey Forum, se ha visto favorecida por la mención específica de la biometría como factor inherente de autenticación según las recomendaciones del BCE, así como la expansión de la huella digital en los dispositivos Apple y Android.

No obstante, quedan todavía algunas incógnitas por despejar. Una de ellas es la estandarización de la biometría y la garantía de seguridad de la información de los usuarios. En este sentido, un programa financiado por la Comisión Europea denominado Biometrics Testing and Evaluation (Test y Evaluación Biométricos, BEAT) tiene como objetivo establecer un marco de evaluaciones operacionales estándar para las tecnologías biométricas con el fin de contribuir al desarrollo de un sistema de certificación de identificación europeo. Esto se logrará a través de:

— El desarrollo de una plataforma *online* abierta para evaluar de forma transparente e independiente los sistemas biométricos con valores de referencia validados.

— El diseño de protocolos y herramientas para el análisis de la vulnerabilidad.

— El desarrollo de documentos de normalización.

El proyecto tendrá fundamentalmente tres resultados relevantes: 1) permitirá medir la fiabilidad de los sistemas biométricos; 2) habrá un marco interoperable, y 3) las empresas y autoridades estarán informadas sobre los avances en el mundo de la biometría que afecten a los estándares.

Por otra parte, queda pendiente resolver el gran enigma de cómo gestionar el robo de información biométrica una vez que se produzca. Actualmente, en el caso de que nos sustraigan o perdamos nuestras contraseñas, la subsanación es tan sencilla como solicitar una nueva, ¿pero qué sucedería si lograsen robarnos la información de nuestra huella dactilar o de nuestro iris? Aunque a priori pueda sonar a ciencia ficción, lo cierto es que ya se han registrado casos de sustracción de información biométrica. En septiembre de 2015, la Oficina de Administración de Personal en Washington sufrió un ciberataque cuya consecuencia, entre otras, fue el robo de 5,6 millones de huellas. Si bien la tecnología contempla elementos adicionales como la temperatura o los poros para evitar suplantaciones, lo cierto es que a día de hoy no sabemos con certeza lo que los ladrones pueden llegar a hacer con la información biométrica hurtada, que, además, es irremplazable para los usuarios.

IV. CONCLUSIONES

La ciberseguridad está en a la agenda de los comités de dirección de las entidades financieras, fundamentalmente debido al incremento de la presión normativa y los cambios legislativos que han ocurrido en el último año. Aunque todavía no se ha instalado totalmente en su ADN hasta el punto de formar parte del núcleo de su responsabilidad empresarial y de su estrategia de transformación digital, se están lanzando iniciativas que van a permitir dar un salto exponencial en sus capacidades e incrementar, por tanto, la confianza digital de sus clientes, entre ellas:

— *Planes de ciberseguridad globales*, orientados de forma práctica a evaluar las amenazas y mitigar el impacto de los riesgos de ciberseguridad en el negocio mediante enfoques basados en Inteligencia de amenazas que difieren en 180º de los planes de seguridad tradicionales.

— *Implementación de procesos de respuesta y defensa activa*, no solo de detección como se ha hecho principalmente en los últimos años, empezando a incluir procesos de orquestación y respuesta automáticos que minimicen el impacto de los ciberataques.

— *Aplicación de tecnologías analíticas* a casos de uso específicos, como por ejemplo análisis de comportamiento para detec-

tar anomalías que incrementen la capacidad de prevención.

Desde el punto de vista de la ciberseguridad, una verdadera transformación digital tiene implicaciones diferenciales en aspectos como la gestión de la identidad digital de sus clientes, la protección de sus activos críticos y la capacidad de predecir las amenazas y tener capacidad de respuesta en tiempo real. El sector financiero es el que está mejor preparado para liderar este proceso y evitar saltos digitales al vacío que puedan dañar de forma irremediable la reputación de una compañía.

Obviamente este es un esfuerzo que debe ser liderado desde la dirección e integrado en los procesos de transformación *top-down*. Realmente creemos que quien sea capaz de integrar la ciberseguridad en sus procesos va a tener una ventaja competitiva diferencial y no tardaremos en verlo en aquellas empresas que adopten este enfoque.

BIBLIOGRAFÍA

Accenture Consulting (2015a), *Biometrics-as-a-Service.*

— (2015b), *Introduction to Biometrics in Financial Services 2015.*

— (2015c), *North America Consumer Digital Payments Survey: When it comes to payments today, the customer rules. Simple. Personal. Everyday.*

Accenture Operations (2015), *Security in Financial Services: Point of View on Digital Identity.*

Accenture Security Services (2015a), *Continuous Cyber Attacks: Engaging Business Leaders for the New Normal.*

— (2015b), *Cybersecurity Strategy and Risk.*

— (2015c), *Estudio de Costes de Tecnologías de la Información en las Entidades Financieras en 2014.*

— (2016), *Defending and empowering the resilient digital business.*

Banco Central Europeo – Eurosistema (2013a), *Recommendations for the security of internet payments.*

— (2013b), *Recommendations for the security of mobile payments.*

Banco de España (2014), *Memoria anual sobre la vigilancia de sistemas de pago.*

Banco Internacional de Pagos (2015), *Statistics on payment, clearing and settlement systems in the CPMI countries - Figures for 2014.*

Diario Oficial de la Unión Europea (2015), *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.*

Kaspersky (2015), *Kaspersky Lab Report: Financial Cyberthreats in 2014.*

Mastercard (2013), *MasterCard Advisors' Cashless Journey: The Global Journey From Cash to Cashless.*

Mobey Forum (2015), *Biometrics in payments: Touching convenience.*

Visa Europe (2015), *Nota de Prensa: Aceptar pagos con tarjeta podría reducir la pérdida de clientes para las pymes en un 24 por 100.*