# Mayor seguridad en las transacciones con tarjetas

**Hoy en día, a nadie se le escapa que el principal medio de pago en todo el mundo es la tarjeta de crédito. Ante el aumento de los fraudes en los últimos años, las entidades emisoras se han unido para crear el estándar PCI DSS, cuya finalidad es aumentar la seguridad de las transacciones financieras.**

DÁMASO VIDAL

Según el barómetro correspondiente al año 2006 realizado por Mastercard, el número de tarjetas en España se ha incrementado un 21% durante los últimos ocho años. Paralelamente a esta cifra, se ha producido un aumento en los fraudes llevados a cabo con este tipo de medio de pago, según confirma la encuesta paneuropea a consumidores encargada por la **European Security Transport Association** (ESTA) hace unos meses. Así pues, el número de españoles que han sido víctimas de fraude con tarjetas de crédito o débito ronda dos millones de personas, lo que supone el 10% de la población adulta. De esta forma, España se sitúa en segundo lugar de la encuesta junto a Francia, y por detrás de Gran Bretaña. En Europa, el número de personas estafadas mediante este medio asciende a 22 millones y el importe anual de fraude en la Unión Europea puede llegar a los tres billones de euros. En nuestro país, según la **Asociación de Usuarios de Servicios Bancarios** (Ausbanc), supera los 12 millones de euros al mes.

Con estos datos sobre la mesa, no resulta extraño que las entidades emisoras de tarjetas hayan iniciado en los últimos años una carrera contra el fraude. Así, las dos principales compañía de este sector, **VISA** y **Mastercard**, desarrollaron a principios de este siglo sus propias iniciativas de seguridad. La primera, mediante los estándares VISA CISP (Cardholder Information Security Program), aplicable en Estados Unidos, y VISA AIS (Account Information Security), para el resto del mundo. La segunda, a través del Mastercard SDP (Site Data Protection). A ellas también se sumaron las compañías **American Express** y **Discover**, con American Express DSOP (Data Security Operating Policy) y Discover DISC (Discover Information Security and Compliance), respectivamente. Sin embargo, ambos proponían recomendaciones de seguridad más simples que las de VISA y Mastercard.

A pesar de este esfuerzo, no se frenaron el número de problemas de seguridad en todo el mundo que presentaban estos medios de pago, por lo que VISA y Mastercard, en colabora-


ción con las organizaciones Discover, American Express y JCB, decidieron alinear sus programas mencionados anteriormente bajo unas únicas directrices: el estándar PCI DSS (Payment Card Industry Data Security Standard), cuyo documento definitivo se publicó en enero de 2005. En palabras de **Daniel Fernández Bleda,** socio y director comercial de la compañía **Internet Security Auditors**, *"el estándar PCI DSS surge a raíz de la gran cantidad de fugas de información relativas a números de tarjetas de crédito a finales de los años 90 y principios de 2000, nacido de la alianza tácita entre dos de los mayores fabricantes en el sector, VISA y Mastercard",* comenta. *"Estas dos compañías", continúa, "se alían a otros como Discover, American Express y JCB en un frente común para demostrar, de cara a la opinión pública, su implicación en proponer soluciones; capacidad de presión sobre aquellas empresas que, de una u otra forma, tratan, transmiten o almacenan datos de todos aquéllos que tiene una tarjeta de VISA o Mastercard; y el esfuerzo en erradicar los escándalos de robos y fugas de tarjetas de crédito que tanto dañan la imagen de los fabricantes, dado que son las marcas que acaban publicándose",* explica el directivo.

A pesar de que han sido estas empresas las que han dado el paso a la hora de elaborar este estándar, cabe hablar de tres principales agentes implicados en el tratamiento de tarjetas. Por un lado, están los *merchants,* empresas que tienen acceso y pueden almacenar datos de cuentas y que deben asegurar esa información y tratarla de forma segura.

A continuación, se encuentran los *service providers*, formados por los Third Party Processor (TPP), vendedores web que contratan a estas entidades para ofrecer sus contenidos y vender sus servicios online; y los Data Storage Entity (DSE), entidades que almacenan y tiene acceso a los datos de las tarjetas. Por último, están los *vendors*, compañías que han pasado los procesos de "homologación" de VISA y Mastercard para ofrecer escaneos de red y auditorías on site y, adicionalmente, análisis objetivos.

En otras palabras, *"PCI DSS no es una norma más para las entidades bancarias, esta asociación suele ser habitual pero incompleta. De hecho, los responsables de cumplimiento de VISA y Mastercard muestran más preocupación en otros sectores que, presumiblemente, pueden parecer no tan concienciados con la seguridad como grandes comercios o empresas que tratan grandes volúmenes de datos de tarjetas de crédito (desde autopistas, empresas de e-commerce, trasmisores de datos de tarjetas, proveedores de servicios que externalizan el tratamiento de datos, etc.)"*, asegura Fernández Bleda. En suma, y tal y como resumen

fuentes consultadas de VISA, *"este nuevo sistema de control y de gestión de las medidas de seguridad en la industria de los medios de pago proporciona unos requisitos de seguridad únicos e iguales para todos los organismos internacionales y para todas las estrategias relacionadas con los medios de pago, lo que mejora la seguridad de la transacción de datos sensibles en el uso de los medios de pago"*. Al respecto, también se pronuncian representantes de BBVA, quienes aseguran que este estándar *"mejora la integridad y seguridad de los medios de pago, por lo que beneficia a todos los intervinientes: entidades bancarias, marcas de tarjetas, comercios y titulares"*.

Fruto de este compromiso de todas las partes implicadas, en septiembre del año pasado se creó PCI SSC (PCI Security Standards Consortium), quien publicó la documentación relativa al estándar y que será de obligado cumplimiento para las entidades que la suscriban a partir de este año. Además, el organismo se encargará, en palabras de los representantes de VISA, *"de gestionar todas las medidas de seguridad disponibles y de acreditar a los organismos que son asesores de seguridad. A través de este organismo también se establecen las directrices básicas que conforman el marco en el que comercios y entidades financieras gestionan esos medios de pago"*, confirman. En este sentido, hay que tener presente que el sector financiero es uno de los más regulados desde el punto de vista de la seguridad, tanto por las normas emitidas por el Banco de España, como por la legislación transpuesta a raíz de directivas europeas. Por lo tanto, las entidades que respalden el estándar deberán contar con *"una implicación mayor, un gran esfuerzo humano y técnico y responsabilidades en la gestión de la seguridad, cosa que pasa por una mayor inversión en seguridad"*, puntualiza Fernández Bleda.

## Obligaciones de las entidades

Sin embargo, esto no es sólo una declaración de intenciones. Es más, el PCI SSC establece una serie de tareas que deben llevar a cabo estas empresas para asegurar su cumplimiento. En primer lugar, se encuentran los análisis propios (Self Assessments), que permiten conocer si la organización incurre en incumplimientos con la norma y el grado. En segundo, están los escaneos de la red (Network Scans), que deben identificar todas las vulnerabilidades que puedan estar presentes en los sistemas. En la versión publicada en 2005 se incide en la diversidad de operativos y sistemas en general. Dentro de esto, se presta mucha atención a la seguridad de las aplicaciones, haciendo hincapié en el seguimiento de recomendaciones de referencia como los de la OWASP (Open Web Application Security Project). Finalmente, están las auditorías internas (OnSite Audit), que implican el cumplimiento de todos los aspectos de la norma. Y es que, como apunta Fernández Bleda, *"aparte de las obligaciones tecnológicas para la mejora e incremento del nivel de seguridad, el estándar obliga a realizar revisiones de seguridad por terceras partes homologadas por el PCI SSC de los Sistemas de Información de las empresas implicadas. Estas auditorías tienen como objetivo garantizar el mantenimiento y gestión de la Seguridad de los Sistemas de Información"*, comenta. Así pues, lo primero que se debe hacer es conocer su estado de seguridad, revisar en detalle la norma y llevar a cabo un análisis diferencial sobre ésta. *"A partir de estos resultados podrá definirse un plan de mejora que debe tener como objetivo la implantación de los controles adecuados para el cumplimiento de todos y cado uno de los requerimientos de forma progresiva"*, añade el directivo.

## Requerimientos

Esos requerimientos a los que se refiere Fernández Bleda están perfectamente detallados. De hecho, el estándar añade una clasificación de las empresas que usan datos de titulares de tarjetas de crédito, así como de las compañías homologadas que deben revisar el cumplimiento de la norma por parte de los primeros. Pero, principalmente, consiste en doce requerimientos globales de seguridad, principalmente técnicos, que conviene conocer.

El primero es el de construir y mantener una red segura. Para ello, es preciso instalar y mantener la configuración del firewall para proteger los datos. La forma de hacerlo es revisando la estructura de la red y la configuración del firewall y otros sistemas de red, incluyendo los inalámbricos; documentar la configuraciones y cambios; revisar el tráfico que puede alcanzar los servidores y que la información no está accesible desde la red externa de forma directa.

El segundo hace referencia a la necesidad de no emplear opciones por defecto en contraseñas y valores de configuración. Al respecto, se deben revisar los sistemas operativos, los servicios de red, los dispositivos de red y filtrado en busca de configuraciones, ficheros, usuarios y contraseñas, etc. por defecto; así como que los servidores no acumulan la prestación de servicios y que éstos emplean soluciones seguras.

El tercero es la protección de los datos almacenados de los usuarios. Para conseguirlo, se hace necesario revisar las políticas y procedimientos de seguridad, el cumplimiento legal vigente (como por ejemplo Ley Orgánica de Protección de Datos) y de las normas de retención y destrucción de los datos de tarjetas. Asimismo, es preciso asegurar que no se almacena ningún tipo de información relativa a las bandas magnéticas, códigos CVV y CVV2 y PINs; y analizar que se emplean métodos válidos de encriptación de información y claves.

El cuarto es la encriptación de las transmisiones de información y datos sensibles de usuarios a través de redes públicas, mediante el análisis de la encriptación adecuada en las aplicaciones web, la revisión de los protocolos de encriptación y la encriptación en la transmisión de información sensible a través de correo electrónico.

El quinto requerimiento que impone el estándar PCI DSS es usar y actualizar regularmente el software antivirus. Es preciso en este sentido comprobar el uso adecuado de software antivirus en los puntos adecuados de la red: ordenadores de usuario, tráfico y servidores de red, correo electrónico, etc.; y revisar la actualización periódica y adecuada de este software.

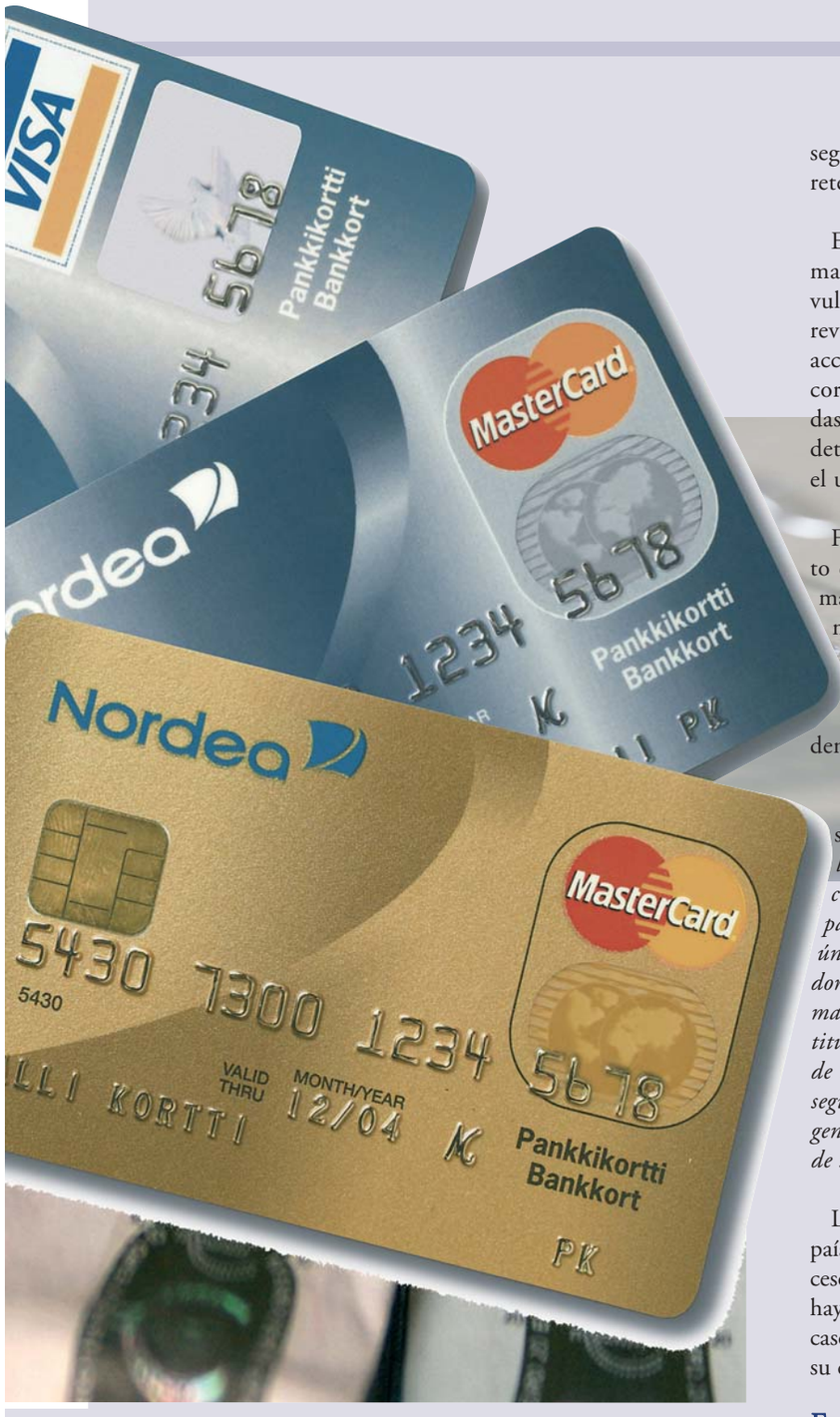
Respecto al sexto, que es el desarrollo y mantenimiento de sistemas y aplicaciones seguras, las organizaciones deben repasar sus políticas de actualización asegurando la aplicación de parches críticos en menos de 30 días, comprobar que disponen de las herramientas y procedimientos adecuados para la identificación de vulnerabilidades, asegurar que cuentan con entornos de desarrollo y producción separados y que la información y las medidas de seguridad adecuadas se aplican en ambos; y, finalmente, asegurarse de que en el desarrollo de las aplicaciones no aparecen vulnerabilidades documentadas por la OWASP.

El séptimo punto es restringir el acceso a los datos. Así, se debe revisar la política de seguridad en busca de la definición de los controles de acceso para todos los sistemas, aplicaciones e información; y la documentación de los sistemas y soluciones para asegurar que permiten implementar los controles de acceso adecuados y se basan en la premisa "deny-all" por defecto.

Asignar un ID único a cada persona con acceso a los sistemas es la octava premisa. En esta ocasión, es preciso comprobar que las personas que acceden a la información de usuarios tienen un ID único, revisar el uso de accesos basados en autenticación de factor-2 en información crítica, asegurar que las contraseñas se almacenan encriptadas, confirmar los procedimientos de asignación y gestión de claves y verificar su robustez; además de auditar todos los sistemas para revisar la implementación de opciones de seguridad en la autenticación.


El noveno requerimiento que impone es restringir el acceso físico a los datos de los usuarios revisando las medidas de seguridad física a los sistemas y la red, sobre todo los que tratan o almacenan datos de usuarios; los sistemas de control de acceso para las visitas; y los registros e instalaciones que almacenan copias de seguridad para comprobar el uso de la seguridad física y sistemas de protección adecuada.

El décimo es la necesidad de auditar y monitorizar todos los accesos a los recursos de red y los datos de usuarios. Para ello, hay que verificar la existencia de la auditoría de eventos de




todo tipo relativos a la información de usuarios, los accesos a la información de auditoría, así como su almacenamiento en copias de seguridad; y revisar que la política de seguridad detalla los aspectos relativos a configuración y retención de datos de auditoría.

El decimoprimero es auditar la seguridad de los sistemas y procesos, asegurando que se realizan escaneos de vulnerabilidades de forma regular. Además, es preciso revisar los procedimientos de búsqueda de puntos de acceso furtivos o dispositivos inalámbricos peligrosos, la corrección de las vulnerabilidades previamente detectadas, el uso, mantenimiento y gestión de sistemas de detección y prevención de intrusiones; así como verificar el uso de sistemas de integridad de ficheros.

Finalmente, el último punto se refiere al mantenimiento de una política que gestione la seguridad de la información, para lo cual se debe comprobar los procedimientos de acciones del día a día en busca de deficiencias en la documentación, asegurar la existencia de un CSO o responsable de seguridad y revisar la documentación de los procedimientos de gestión de incidentes en la empresa.

En total, todos ellos, según las fuentes de VISA consultadas, se dirigen principalmente *"a los comercios y a las entidades financieras que permiten el uso y la aceptación de las tarjetas en las terminales del punto de venta para conseguir aunar sus propios intereses en un objetivo único, la correcta gestión de la información de los consumidores. Esto se consigue estableciendo y manteniendo un sistema de seguridad de datos, protegiendo la información de los titulares de las tarjetas, mejorando los programas de gestión de datos, implementando fuertes medidas de control de la seguridad, analizando y estudiando las incidencias que surgen y, sobre todo, asegurando el correcto uso de las políticas de seguridad de la información"*, explican.

Lo que sucede es que España todavía no se considera un país crítico de acción. De hecho, no se están abriendo procesos de certificación de empresas ni auditores, puesto que hay pocas compañías clasificadas de Nivel 1. En cualquier caso, sí que las entidades pertinentes están trabajando para su cumplimiento e implantación sea la mayor posible.

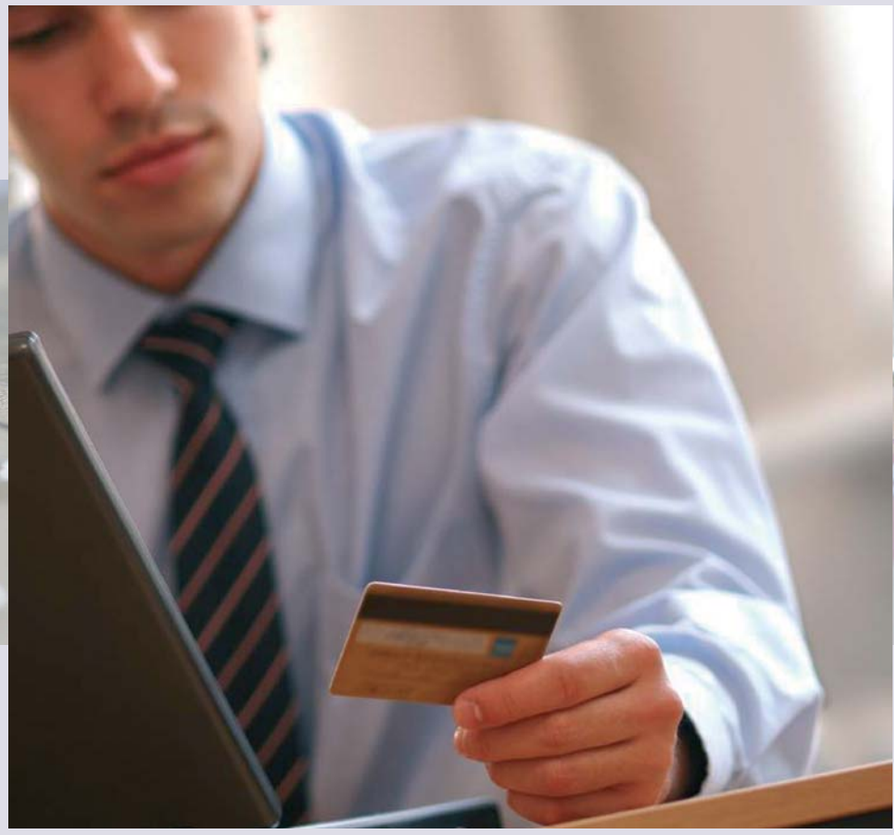
## Evolución de los medios de pagos

Aunque la influencia en los medios de pago de una norma como PCI DSS es nula, puesto que *"no es un docu-* ▶▶

### SINGLE EURO PAYMENTS AREA

La Zona Única de Pagos para el Euro (SEPA, Single Euro Payments Area) es una realidad que será operativa desde inicios de 2008 y reemplazará completamente los sistemas de pagos nacionales. Esta iniciativa se gestó en las instituciones europeas con la finalidad de alcanzar mayores niveles de eficiencia en las crecientes transacciones comerciales europeas. Por eso, la banca se ha estado preparando y ha previsto reducciones muy significativas en sus márgenes. La estandarización del sistema de cobros y pagos facilitará en gran medida un tratamiento administrativo unificado y eficiente de nuestras transacciones comerciales europeas, lo que facilitará reconciliaciones, pero requerirá depurar datos de clientes y proveedores eliminando sistemas de pagos obsoletos. Sin embargo, hasta el momento, las empresas, beneficiarias finales de todo el esfuerzo, se han mantenido al margen de la iniciativa.

*mento que modifica o implica una evolución de éstos sino que regula o mejora cómo se opera con los existentes"*, según Fernández Bleda, sí es justo reconocer que va a suponer un importante avance para mejorar la seguridad en las transacciones financieras.



Precisamente, sobre esta base se asentarán los estándares EMV (creado por Europay International, MasterCard International y Visa International,) o las futuras medidas de pago electrónico europeas Single Euro Payments Area (SEPA), que tendrán su inicio el 1 de enero de 2008. "El primero en la utilización de tarjetas, cajeros, lectores y componentes de pago en general más seguros, y los segundos en la unificación de los procedimientos e información de los datos de pago para agilizar la transferencia de información y, presumiblemente, reducir el fraude del pago electrónico y que pretende incluso sustituir a SWIFT como método de transferencia internacional de capitales", afirma el directivo.

Esto, por supuesto, se encuentra en concordancia con las metas que se han propuesto desde VISA: *"Nuestro objetivo", comentan fuentes de la compañía, "es sustituir gradualmente otras formas de pago (por ejemplo el efectivo y los cheques) por pagos electrónicos más rápidos, seguros y cómodos". De hecho, ya se encuentran trabajando con ciertas entidades asociadas españolas para crear un mercado de pagos electrónicos más grande, abierto, dinámico y competitivo. "La implantación de la primera infraestructura de pagos con chip del mundo", continúan, "el desarrollo de una solución paneuropea de tarjetas de débito basadas en chip, proporcionar mayor comodidad y confianza en el comercio electrónico y crear un nuevo sistema europeo de procesamiento de transacciones son algunas de las iniciativas e innovaciones actuales".* Por supuesto, a la realización todas estas medidas pueden contribuir la implantación y el cumplimiento del estándar PCI DSS. ■

## EMVCO, LA ORGANIZACIÓN DE ESTÁNDARES PARA TARJETAS INTELIGENTES

Constituida en febrero de 1999 por Europay International, MasterCard International y Visa International, esta entidad se encarga de de la gestión, mantenimiento y mejora de las Especificaciones de los Circuitos Integrados en las Tarjetas para Sistemas de Pago EMV. Con la adquisición de Europay por parte de MasterCard en 2002 y la unión de JCB, hoy en día, EMVCo está constituido por JCB, Mastercard y VISA. El principal objetivo de la organización es el mantenimiento de los estándares, que sirven para asegurar la interoperabilidad y aceptación de los sistemas de pago integrados en los circuitos de las tarjetas y en las aplicaciones de pago a nivel mundial.

Las especificaciones EMV, desarrolladas en principio conjuntamente por las tres organizaciones, definen una serie de requisitos que garantizan la interoperabilidad de aplicaciones de pago de crédito y débito entre tarjetas inteligentes y terminales en una base global, con independencia del lugar en el que se utilice la tarjeta. Estas especificaciones sirven de marco para fabricantes de tarjetas inteligentes y terminales de todo el mundo. A medida que la tecnología avanza y se extiende la implantación de programas con tarjetas inteligentes, EMVCo garantizará que se desarrolle un proceso de aprobación en un solo terminal a un nivel que permitirá la interoperabilidad de sistemas de pago cruzado gracias a la compatibilidad con las especificaciones EMV. En este sentido, la organización establece un calendario que, dependiendo de las zonas, todas las tarjetas de débito o crédito deberán ser tarjetas inteligentes, reemplazando a las de banda magnética actuales.