PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

GoNet
Fraud Prevention
& Intelligence

Mayo 2018

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

Los sistemas de pagos online evolucionan casi a la misma velocidad que se adoptan e implementan. El uso de dispositivos móviles ha incrementado la preocupación sobre la seguridad de los pagos digitales, especialmente en lo que a la privacidad y confidencialidad de la información financiera se refiere.

Cada día se realizan ingentes cantidades de operaciones financieras a través de internet, no sólo compras, sino pagos de facturas y todo tipo de transacciones bancarias. Todas estas operaciones crean una gran cantidad de datos confidenciales que se deben proteger, por eso la implementación segura de un sistema

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

La normativa PDI DSS se aplica a cualquier organización, independientemente del tamaño o número de transacciones, que acepte, transmita o almacene datos de tarjetas de crédito

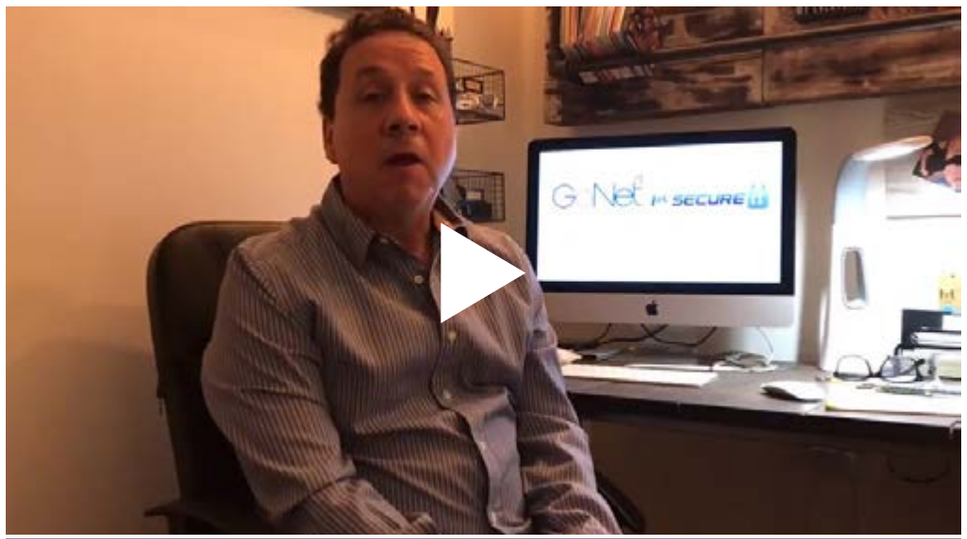
de pago de comercio electrónico debe incluir la posibilidad de identificar robos y todo tipo de fraudes online.

Precisamente el que los casos de fraude con las tarjetas de pago crecieran de forma alarmante fue lo que llevó en 2006 a las empresas de tarjetas más importantes, como American Express, Discover, JBC, Mastercard y VISA, a unirse para crear el PCI-SSC (Payment Card Industry – Security Standard Council), que sirvió para la creación del estándar conocido como PCI-DSS (Payment Card Industry – Data Security Standard), que no es otra cosa que un conjunto de requerimientos cuyo objetivo es asegurar que todas las compañías que procesan, almacenan o transmitan información sobre tarjetas de crédito cuenten con un entorno seguro.

Se entiende por información de tarjeta el número PAN completo (es el número de 16 dígitos que se encuentra al frente de la tarjeta), el nombre del propietario de la tarjeta, la fecha de expiración y el código de servicio (código de 3 o 4 dígitos que se encuentra en la banda magnética). En todo caso, adicionalmente son considerados datos sensibles el código de seguridad (CVC o CVV), la información completa de la banda magnética (o el equivalente en las tarjetas chip) y los PINs, ya que estos datos son los que se utilizan como códigos de autenticación para autorizar las transacciones de pago.

Muchos comercios creen que la implantación de sistemas de pago tokenizados, o que cumplen la norma P2PE, les exime del cumplimiento de la normativa, cuando no es así, aunque esto facilita mucho el cumplimiento. Las verticales objetivo de cumplir con PCI DSS son: Retail (online/offline); Call centers (solo aquellos que acepten pagos por teléfono o email); Banca (aquellos que trabajen con comercios); Finanzas; Agencias de viajes (obligado cumplimiento desde el 1 de marzo de 2018); Proveedores de medios de pago y afines.

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance



En todo caso, la normativa PDI DSS se aplica a cualquier organización, independientemente del tamaño o número de transacciones, que acepte, transmita o almacene datos de tarjetas de crédito. Lo que sí que varía es el modo en que el cumplimiento es auditado, en función de la cantidad de transacciones anuales que la organización realice. Se establecen cuatro niveles, siendo el primero el asociado a todas las organizaciones que procesen más de seis millones de transacciones anuales, que serían auditadas por una empresa auditora habilitada por el consorcio PCI.

Cumplir con los estándares de seguridad PCI puede parecer una tarea desalentadora, pero el cumplimiento es cada vez más importante y puede no ser tan problemático si se cuenta con las herramientas y, por supuesto, con los socios y los asesores adecuados. Además, el coste de no cumplir con la normativa se ha disparado y puede suponer una cantidad muy elevada. Un reciente estudio elaborado por Ponemon Institute y titulado The True Cost of Compliance with Data Protection Regulations, recoge que los costes en los que puede incurrir una empresa que no cumpla con normativas relacionadas con la protección de datos ha crecido un 45% respecto a 2011, alcanzando los 14,82 millones de dólares anuales. Por otra parte, y aunque la mayoría de encuestados hicieron referencia a GDPR, un 55% consideró que el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago es un desafío.

Adoptar PCI DSS no sólo evita problemas de incumplimiento normativo, sino que ofrece una serie de ventajas:

- La primera y principal es que los sistemas son seguros y los clientes pueden confiar la empresa.
- Mitigar los riesgos asociados a un posible compromiso de la información de cuentas o titulares de tarjetas, reduciendo los costes legales y el impacto negativo en la imagen.

El número de españoles con al menos una tarjeta en su posesión alcanzó en 2017 al 82% de la población

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

¿Qué preocupa a los clientes?

Los tres problemas a los que se enfrentan los clientes a la hora de cumplir con la normativa PCI DSS y que la solución de GoNetFPI y 1st Secure IT resuelve son:

- MINIMIZAR EL ALCANCE DE LA NORMATIVA PARA SU ENTORNO IT, lo que implica reducir tanto económica como temporalmente el proceso de certificación.
- MINIMIZAR LA EXPOSICIÓN A POSIBLES BRECHAS DE SEGURIDAD, lo que reduce significactivamente el riesgo de aparecer en medios de comunicación y por tanto la erosión de su imagen en el mercado.
- POSIBLES SANCIONES POR EL INCUMPLIMIENTO DE LA NORMA por parte de las marcas y tarjetas (VISA, Mastercard, JCB, Discover y AMEX).

- El cumplimiento de PCI mejora su reputación no sólo de cara a los compradores, sino a las marcas de pago.
- El cumplimiento de PCI es un proceso continuo que ayuda a prevenir las violaciones de seguridad y el robo de tarjetas de pago, ahora y en el futuro.
- Seguir los estándares de PCI DDS ayuda también a estar cerca de cumplir con otras regulaciones adicionales, como HIPAA o SOX.
- El cumplimiento de PCI contribuye a las estrategias de seguridad corporativas.
- El cumplimiento de PCI probablemente conduzca a mejorar la eficiencia de la infraestructura de TI.
- En el caso de los proveedores de servicios, el cumplimento de PCI DSS constituye un elemento diferenciador que puede suponer una ventaja competitiva en el mercado.
- La implementación de buenas prácticas de seguridad en la compañía recogidas en la norma.

Los grandes retos de PCI DSS

Aunque todos los comerciantes y proveedores de servicios que almacenan, procesan o transmiten datos de titulares de tarjetas deben cumplir con el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), la realidad es que muchos no lo hacen. De hecho, los datos muestran que las empresas inicialmente cumplen entre el 18% a 24% de la norma.

A veces el problema está en el alcance de la propia norma. El estándar tiene 243 requisitos numerados y 330 requisitos de prueba que todos los comerciantes deben cumplir. La mayoría de las organizaciones que admite IT Governance están clasificadas como Visa o MasterCard Nivel 3 o Nivel 4 para fines de informes. Estas organizaciones generalmente informan de su cumplimiento mediante un cuestionario de autoevaluación (SAQ). Si bien el objetivo de los SAQ es simplificar el proceso de notificación de cumplimiento, a menudo las compañías tienen dificultades para cumplimentarlo. También suelen subestimar qué partes de su entorno deben cumplir y cómo proteger esos sistemas.

Otro de los principales problemas es la conciencia de seguridad continuada. La protección de datos no se trata solo de usar cifrado, firewalls y software antivirus. También se trata de un proceso continuo de monitorización, de mantenimiento y gestión de la configuración, de administración de identidades, registro, escaneo y pruebas continuas. Lo que queremos decir con esto, es que muchas organizaciones no cumplen con los requisitos porque no reconocen la importancia de realizar pruebas regulares. Y hay que recordar que el requisito 11 de PCI DSS descri-

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

be la necesidad de llevar a cabo pruebas periódicas para identificar problemas de seguridad no abordados.

Otro de los retos de la normativa es la necesidad de realizar una revisión diaria de los eventos y registros de seguridad, como pueden ser las cuentas y actividad de las personas asociadas con la información de la red, establecido en el requisito 10.6.1. Mantener soluciones de registro puede hacer que el porcentaje de cumplimiento con PCI de una organización se reduzca, ya sea por restricciones técnicas, presupuestarias o de recursos humanos. En todo caso, no significa que el estándar pueda ser ignorado, entre otras cosas porque las organizaciones que no cumplen con los requisitos podrían incurrir en fuertes multas. Para evitar esto, las organizaciones deben reconocer los desafíos de cumplir con las PCI DSS y encontrar la manera de superarlas.

> Muchos comercios creen que la implantación de sistemas de pago tokenizados, o que cumplen la norma P2PE, les exime del cumplimiento de la normativa, cuando no es así

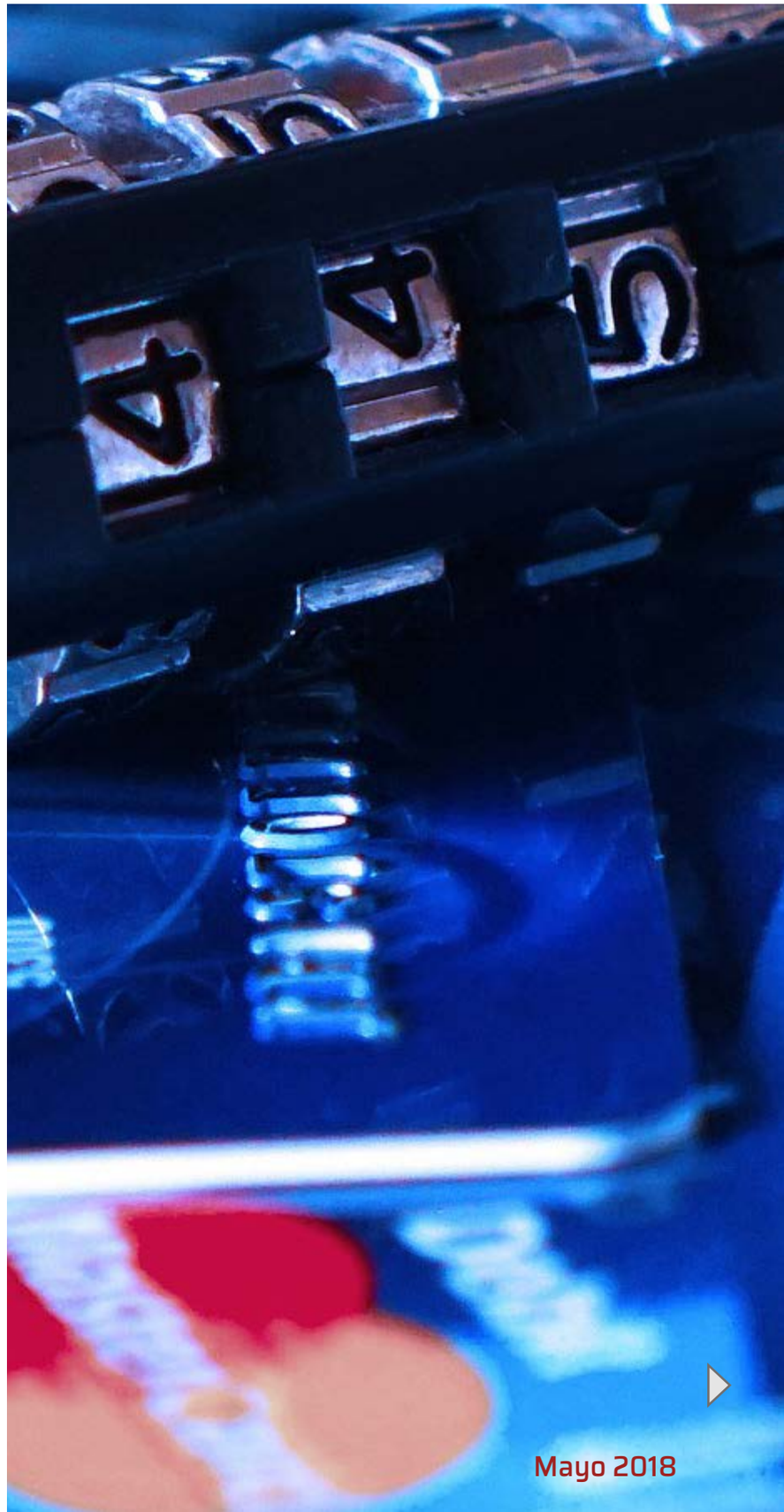
Proteger los datos almacenados de las tarjetas es otro gran reto para muchas empresas. Decíamos que, como mínimo, el estándar requiere que el número de cuenta principal (PAN) se vuelva ilegible en cualquier lugar donde esté almacenado, incluidos medios digitales portátiles, medios de respaldo y registros.

Hay que tener en cuenta además que las aplicaciones normalmente son propiedad del banco que exige el cumplimiento, lo que hace responsable a los comercios y Service Providers de desarrollo de Normativa de Seguridad, identificación y autenticación de usuarios, gestión de pistas de auditoría, identificación de vulnerabilidades y gestión de actualizaciones y pruebas de intrusión.

Alianza GoNetFPI y 1st Secure IT

GoNetFPI y 1st Secure IT se unen para luchar contra el fraude en medios de pago en el mercado ibérico mediante una alianza que permite ofrecer la máxima seguridad a sus clientes que operen con medios de pago tanto en el mercado ibérico como en el europeo y latinoamericano. Para ello, la alianza cuenta con un equipo dedicado en exclusiva a esta actividad y que está apoyado en todo momento por un grupo con más de 20 expertos auditores internacionales certificados como QSA por el PCI Council.

El número de españoles con al menos una tarjeta en su posesión alcanzó en 2017 al 82% de la población, lo que se tradujo en un aumento de ocho puntos porcentuales en relación al dato registrado un año antes y supone el dato más alto de toda la serie histórica desde hace 30 años, según una encuesta



PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

Compartir en RRSS

realizada por Mastercard. Actualmente en el mercado ibérico hay más tarjetas que habitantes de ahí que sean uno de los focos de los ciberdelincuentes y la necesidad de proteger las operaciones que se realizan con las mismas. La ciberdelincuencia ha encontrado uno de sus nichos y de ahí la importancia de ofrecer los servicios más completos y seguros para proteger los medios de pago de posibles ataques.

El objetivo de esta colaboración entre GoNetFPI y 1st Secure IT es atender a cualquier tipología de clientes que opere con medios de pago, desde comercios electrónicos, agencias de viajes hasta agregadores, procesadoras o entidades financieras, ya sean emisoras o adquirentes, cubriendo todas sus necesidades desde la certificación PCI, hasta el análisis de negocio y la gestión de riesgos.

GoNetFPI y 1st Secure IT ofrecerán sus capacidades en la certificación de PCI (Payment Card Industry) en el mercado europeo, con un primer foco de entrada en España y Portugal, donde el uso de tarjetas para realizar los diferentes pagos es la práctica más habitual.

1st Secure IT destaca en el sector de la ciberseguridad por realizar certificaciones PCI-DSS desde hace más de una década en Estados Unidos y Latinoamérica, entornos que han cambiado mucho en los últimos años. La compañía, con oficinas en Florida, Massachusetts, Brasil y México D.F., apoya a las instituciones, convirtiéndose en su aliado durante todo el proceso, para mejorar su seguridad en el procesamiento de datos y lograr cumplir con el estándar PCI-DSS de una manera práctica, sencilla y eficiente.

Tanto en España, como en Europa y a nivel mundial, la oferta de GoNetFPI y 1st Secure IT se diferencia de la competencia por la realización de GAP Analysis gratuito para nuevas contrataciones del servicio; mínima presencia on-site de los asesores de la compañía utilizando herramientas colaborativas y contar con más de 20 asesores a nivel mundial.

Enlaces de interés...

- GoNetFPI
- PCI-DSS Compliance
- GoNetFPI y 1st Secure IT se unen en la lucha contra el fraude en medios de pago