Getnet
By Santander

Guía de cumplimiento básica PCI DSS

Índice Interactivo

La vulneración de los datos de las tarjetas de pago de tus clientes tiene un efecto inmediato en tu negocio: daños reputacionales, pérdida de confianza, sanciones y otras muchas consecuencias que pueden perjudicar tu empresa. El número de configuraciones y funcionalidades en los medios de pago cada vez es mayor, y en caso de no hacer un uso adecuado de las mismas, se puede convertir en un punto débil que facilite el acceso a los datos de los clientes. Por ejemplo, tecnología Wifi, software de acceso remoto o sistemas de grabación, entre otros.

Por ello, es importante que se tengan en cuenta algunos conceptos que son necesarios para cumplir con los estándares de seguridad obligatorios para todos los comercios. A continuación, enumeramos los citados conceptos básicos.

1 | ¿Qué significa PCI?

Los PCI DSS ("PCI" es el acrónimo de Payment Card Industry y "DSS" se refiere a Data Security Standard) son los estándares de seguridad que tienen que cumplir todos los comercios o proveedores de servicios que procesan o almacenan datos de tarjetas. Se trata de un **conjunto de requisitos técnicos y operativos que se crean para proteger los datos de los titulares de tarjeta.**

El organismo PCI SSC (Security Standards Council), que ha sido creado por las principales marcas internacionales, es el responsable de establecer los referidos estándares de seguridad que aplican a todos los participantes en el sector (entidades financieras, comercios, proveedores de servicios, empresas de software, entre otros).

2 | ¿Por qué se debe cumplir con PCI DSS y cuáles son las consecuencias del incumplimiento?

Es fundamental asegurarnos que los datos de las tarjetas de nuestros clientes están completamente protegidos. Y para ello, es necesario saber que:

- **Proteger los datos** nos ayuda a evitar los fraudes asociados a las brechas de seguridad que pueden producirse en el sistema, así como los "compromisos de datos". Es decir, cualquier tipo de acceso ilegítimo a los datos de las tarjetas de nuestros clientes.

- **Se debe evitar la pérdida de confianza** de nuestros clientes, ya que éstos presuponen que los datos de su tarjeta están seguros en todo momento y en cualquier sistema.

- **Se pueden derivar daños hacia la marca,** el adquirente y en mayor medida para el comercio en el caso de que se produzca un acceso ilegítimo de los datos, lo que puede tener consecuencias económicas, de imagen o reputacionales, lo que supondría poner en peligro su negocio.

- **Las técnicas de las organizaciones criminales se perfeccionan** con el tiempo y cada vez tienen más medios para acceder a los sistemas de los comercios. Por ello, es importante cumplir con los requisitos técnicos y de seguridad para evitar intrusiones.

Y, ¿qué ocurre si el comercio no cumple con los estándares PCI DSS? Este incumplimiento puede acarrear graves consecuencias, entre las que destacan:

Pago de multas o sanciones impuestas por las marcas o incluso por los adquirentes, así como el posible pago de indemnizaciones a los clientes que han sido afectados , ya que el titular de la tarjeta en ningún caso asume los cargos realizados y no reconocidos como propios. También conllevaría la asunción de otros costes como los de las investigaciones forenses (denominadas PFI) o de las acciones correctivas (ya que son mayores a los implementados de forma preventiva).

Imposibilidad de trabajar con el adquirente porque debe garantizar que todos los comercios adquiridos cumplen con dichos estándares para no incurrir en riesgo reputacional, económico o de sanciones.

Posibilidad de incurrir en el incumplimiento de otras leyes y normativa.

3 | ¿Qué acciones debo llevar a cabo para cumplir con PCI?

Si queremos proteger los datos de nuestros clientes es necesario:

1. **Desarrollar y mantener una red segura.**
2. **Proteger los datos** almacenados de los propietarios de tarjetas, cifrar los datos y demás información confidencial transmitida a través de redes públicas abiertas.
3. Mantener un programa de **gestión de vulnerabilidades** (utilización y mantenimiento de antivirus y aplicaciones seguras).
4. Implementar medidas sólidas de **control de acceso** (restricciones de acceso, identificaciones únicas)
5. **Monitorizar y probar regularmente las redes.**
6. **Mantener una política de seguridad de la información.**

Y para ello, la buena noticia es que puedes comenzar a proteger tu negocio hoy mismo con estos conceptos básicos de seguridad:

Usa contraseñas seguras y cambia las predeterminadas

Coste
Facilidad
Mitigación de los riesgos

Protege los datos de las tarjetas y almacena únicamente lo que necesites

Coste
Facilidad
Mitigación de los riesgos

Inspecciona los terminales de pago para detectar manipulaciones

Coste
Facilidad
Mitigación de los riesgos

Recurre a socios comerciales de confianza y aprende a contactar con ellos

Coste
Facilidad
Mitigación de los riesgos

Instala parches de tus proveedores

Coste
Facilidad
Mitigación de los riesgos

Protege el acceso interno a los datos de las tarjetas

Coste
Facilidad
Mitigación de los riesgos

No permitas que los piratas informáticos accedan fácilmente a tus sistemas

Coste
Facilidad
Mitigación de los riesgos

Usa software antivirus

Coste
Facilidad
Mitigación de los riesgos

Realiza análisis en busca de vulnerabilidades y soluciona los problemas

Coste
Facilidad
Mitigación de los riesgos

Utiliza terminales y soluciones de pago seguro

Coste
Facilidad
Mitigación de los riesgos

Protege tu negocio en Internet

Coste
Facilidad
Mitigación de los riesgos

Para una protección óptima, haz que tus datos sean inútiles para los delincuentes

Coste
Facilidad
Mitigación de los riesgos

Además de estas indicaciones, en función del nivel de PCI que ostente el comercio, se derivarán otras obligaciones, como la presentación de diferentes documentos y realización de auditorías. A continuación, se exponen de manera sencilla:

¿Qué nivel de PCI tiene mi comercio?

Para cumplir con todos los requerimientos de seguridad, existen niveles de PCI para los comercios, en función de los cuales se les asignan una serie de documentos requeridos por las marcas para validar el nivel de cumplimiento.

Nivel 1: Comercios que procesan más de 6 millones de transacciones anuales (documentos: ROC, AOC y ASV).
Nivel 2: Comercios que procesan entre 1 y 6 millones de transacciones anuales (documentos: SAQ, AOC y AV).
Nivel 3: Comercios que procesan entre 20.000 y 1 millón de transacciones anuales de comercio electrónico (documentos: SAQ y AOQ)
Nivel 4: Comercio electrónico que procese menos de 20.000 transacciones y el resto de comercios que realicen menos de 1 millón de transacciones (documento: SAC)

¿En qué consiste cada documento?

- **ROC** (Report on Compliance): es un informe en el que se acredita el cumplimiento de las normas PCI. La auditoría PCI DSS a un comercio nivel 1, se podrá realizar con un asesor externo (QSA) o interno (ISA) cualificado. En el caso de los proveedores de servicio, la auditoría sólo puede ser realizada por un asesor externo.
- **SAQ** (self-assessment questionnaire): es un documento de autoevaluación para comercios y proveedores de servicio, en el que se dejará constancia del grado de cumplimiento de PCI DSS. En función de la tipología de comercio le aplicarán unos controles u otros.
- **AOC** (Attestation of Compliance): es una declaración de cumplimiento que contiene una versión simplificada del SAQ o el ROC.
- **Escaneos por un ASV** (Approved Scanning Vendor): Se trata de análisis internos y externos de las vulnerabilidades de la red de forma trimestral realizados por una empresa homologada por el PCI SSC como ASV.