CLOUDFLARE

DOCUMENTO TÉCNICO

Un enfoque estratégico para garantizar la conformidad normativa de PCI DSS 4.0

Contenido

Información general

Todas las organizaciones que procesan tarjetas de crédito, débito o prepago deben cumplir los estándares de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI), como pequeños comercios, minoristas, sitios web de comercio electrónico, bancos y grandes empresas. Sin embargo, la migración a la nube y la adopción del trabajo híbrido, junto con la evolución de los estándares conforme se implementa la nueva versión PCI DSS 4.0, dificultan la conformidad de forma eficiente.

Se necesita un nuevo enfoque para este mundo modernizado digitalmente, que agilice el proceso de conformidad de forma escalable, permitiendo a las organizaciones mantenerse a la vanguardia con el panorama normativo dinámico y seguir el ritmo de la modernización digital de las empresas.

Desafíos de la conformidad normativa de PCI DSS para las organizaciones de hoy día

La conformidad de la normativa PCI es crucial, ya que los infractores se exponen a sanciones, demandas judiciales e investigaciones gubernamentales. Sin embargo, la conformidad presenta varios desafíos para las instituciones financieras, los comercios electrónicos y otras empresas sujetas a su normativa.

Además, como los equipos de informática han perdido el control de sus entornos digitales debido a una mayor dependencia de la informática en la nube y el teletrabajo, el proceso de resolución de esos desafíos se ha vuelto más complejo.

Asignación de tiempo y recursos: el 53 % de las organizaciones afirma que no hay personal suficiente que pueda desempeñar puestos técnicos especializados en privacidad, lo que dificulta garantizar la conformidad.[1]

Seguridad de los datos en entornos diversos: con el auge de la informática en la nube y los pagos móviles, velar por la conformidad en entornos diversos y a menudo menos controlados es cada vez más difícil.

Complejidad con la integración de la pila tecnológica: la integración y el mantenimiento de las tecnologías necesarias para cumplir las normas de conformidad, como las configuraciones de la encriptación y los firewalls, suelen ser complejos. Este desafío se agrava en organizaciones con sistemas heredados o en procesos de transformación digital.

Auditoría: los equipos informáticos deben mantener un registro de auditoría actualizado en toda la infraestructura y los sistemas para garantizar la conformidad.

Conformidad de proveedores: garantizar que los proveedores de servicios y vendedores externos cumplan los estándares PCI añade complejidad.

Cómo mantenerse a la vanguardia de las ciberamenazas sofisticadas

La versión 4.0 del estándar PCI DSS se publicó el 31 de marzo de 2022 y entró en vigor el 31 de marzo de 2024 (los requisitos adicionales lo harán justo un año después). Los objetivos de la versión PCI DSS 4.0 son:[2]

1. **Seguir respondiendo a las necesidades de seguridad de la industria de tarjetas de pago**

- **Mejora de los requisitos de autenticación:** se hace mayor hincapié en la autenticación, sobre todo en la autenticación multifactor para todos los accesos al entorno de datos del titular de la tarjeta (CDE). Los requisitos de contraseña también son más estrictos, pasando de 8 a 12 caracteres como mínimo.
- **Requisitos de encriptación más estrictos:** PCI DSS 4.0 exige el uso de una encriptación "segura" para el almacenamiento y la transmisión de los datos de los titulares de tarjetas, como el protocolo TLS que no es vulnerable a amenazas conocidas.
- **Nuevos requisitos relativos al comercio electrónico y al phishing para hacer frente a las amenazas actuales:** la versión 4.0 incluye nuevos requisitos para la seguridad del lado cliente y para la protección contra el phishing y la ingeniería social.

2. **Promover la seguridad como proceso continuo**

- **Mayor atención al análisis y la gestión de riesgos:** se anima a las organizaciones a implementar procesos continuos de análisis y gestión de riesgos para identificar y abordar las vulnerabilidades con rapidez.
- **Mayor énfasis en la responsabilidad y la gobernanza:** la nueva versión hace más hincapié en la gobernanza de los datos de los titulares de tarjetas y en la responsabilidad de mantener los controles de seguridad.
- **Mayor orientación para implementar y cumplir los requisitos de seguridad:** la versión 4.0 de PCI DSS aclara la intención de la norma y los plazos utilizados.

3. **Añadir flexibilidad para diferentes metodologías**

- **Integración de nuevas tecnologías:** la versión 4.0 aborda la seguridad de las tecnologías emergentes como los sistemas de pago en la nube y móviles.
- **Mayor flexibilidad para la forma en que las organizaciones pueden alcanzar los objetivos de seguridad:** las organizaciones pueden utilizar un "enfoque personalizado", una mayor variedad de métodos para cumplir la normativa. La versión PCI DSS 4.0 ofrece más flexibilidad para establecer la frecuencia con la que realizan acciones basadas en análisis de riesgos específicos.

4. **Mejorar los métodos de validación**

- **Supervisión y pruebas continuas:** la nueva normativa fomenta un cambio de la validación anual de la conformidad a la supervisión continua de la seguridad y la conformidad.
- **Mayor alineación entre las evaluaciones y los certificados de conformidad:** la información de los cuestionarios de autoevaluación o de los informes de cumplimiento está más alineada con lo que se resume en las certificaciones de conformidad.

Solución: Un nuevo enfoque para garantizar la conformidad con la normativa PCI a través de la conectividad cloud de Cloudflare

Los equipos de informática y de seguridad necesitan abordar los requisitos de la PCI de una forma sencilla y programable que se integre fácilmente con su pila actual de seguridad y de tecnología, y que siga haciéndolo a medida que evoluciona tanto su infraestructura como la normativa PCI DSS.

La respuesta no está en planteamientos confusos que incluyan muchas soluciones de seguridad específicas y heredadas. En su lugar, los equipos necesitan una plataforma unificada de servicios de seguridad y redes nativos de nube diseñados para ayudar a las empresas a recuperar el control de sus entornos informáticos y cumplir diversos requisitos de conformidad, incluida la PCI. Dicha plataforma unificada se denomina conectividad cloud.

La conectividad cloud de Cloudflare ofrece:

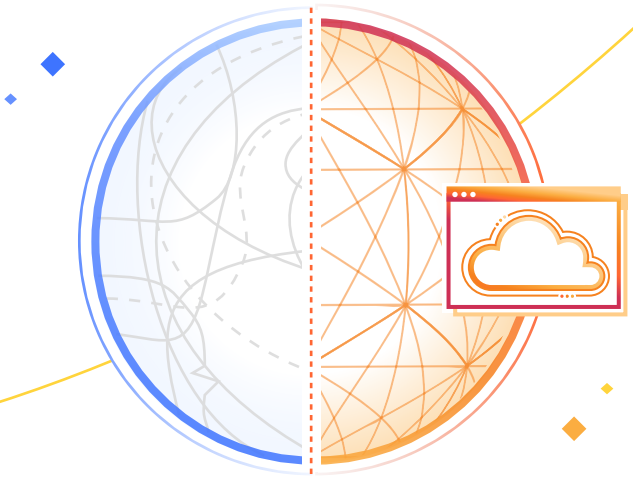
- Una plataforma diseñada para la conformidad de datos
- Un motor de políticas unificado
- Soberanía de datos sin concesiones
- Elaboración de informes inteligentes para satisfacer las auditorías

Cloudflare permite a los equipos de informática aplicar controles coherentes en todas las ubicaciones, utilizando un único panel de control para activarlos en todas partes.

Los equipos pueden enviar registros directamente desde el perímetro de Cloudflare a su SIEM preferido o a un destino en la nube para su auditoría. Además, la visibilidad a gran escala del tráfico de Internet de Cloudflare permite la identificación y la protección automáticas contra nuevas amenazas.

Cloudflare cumple la normativa PCI y es compatible de forma nativa con los requisitos PCI DSS 4.0. Por ejemplo, Cloudflare permite a los equipos de informática aplicar fácilmente la autenticación multifactor, uno de los puntos principales del estándar PCI DSS 4.0. Cloudflare también es compatible con los últimos estándares de encriptación y a menudo contribuye a ellos, ayudando a los clientes a cumplir los requisitos de los estándares PCI DSS 4.0 para la encriptación de información confidencial.

En la página siguiente encontrarás un resumen de los requisitos de la normativa PCI DSS y las capacidades de la conectividad cloud de Cloudflare:



Áreas clave en las que Cloudflare puede ayudar a cumplir los requisitos de la normativa PCI*

Requisitos de la normativa PCI	Capacidades de Cloudflare
1. Instalar y mantener controles de seguridad de red (anteriormente "instalar y mantener un firewall").	Cloudflare protege redes, aplicaciones e implementaciones en la nube por igual del tráfico de red malicioso. Cloudflare utiliza la información sobre amenazas de cientos de miles de millones de amenazas diarias para proteger los sitios web y las aplicaciones web de las amenazas, incluidas las 10 principales vulnerabilidades de OWASP y los ataques de día cero. Su plataforma de seguridad es nativa de nube, se implementa en minutos y permite a los usuarios aplicar cambios de políticas globales en segundos.
2. Aplicar configuraciones seguras a todos los componentes del sistema.	La protección que brinda Cloudflare a usuarios, dispositivos y aplicaciones se basa en técnicas de encriptación y enmascaramiento frente a posibles atacantes en la web. La solución API Shield de Cloudflare permite a los usuarios crear medidas de protección contra vulnerabilidades en sus API identificando secuencias y aplicando políticas en torno a las transacciones API.
3. Proteger los datos almacenados mediante la encriptación u otros métodos de protección de datos.	Cloudflare puede identificar información de identificación personal (IIP) en reposo, y cumple los requisitos relacionados con el tiempo de conservación de registros de titulares de tarjetas.
4. Encriptar los datos de los titulares de tarjetas en redes públicas abiertas.	El tráfico enviado a través de la red global de Cloudflare cumple las normas de encriptación especificadas en este requisito. Asimismo, Cloudflare puede bloquear la transmisión de la IIP que el usuario necesita identificar.
5. Proteger todos los sistemas y redes del software malicioso.	Cloudflare atiende más de 55 millones de solicitudes HTTP por segundo, lo que nos proporciona una visión única de gran alcance de los últimos ataques en el entorno. Cloudflare proporciona a los usuarios un conjunto de soluciones de protección antimalware como antivirus, seguridad del correo electrónico en la nube y aislamiento remoto del navegador.
6. Desarrollar y garantizar la seguridad de los sistemas y el software.	Cloudflare puede clasificar y evaluar las infracciones de seguridad de los usuarios, así como los errores de configuración que detecta en las aplicaciones SaaS. Los servicios de seguridad de Cloudflare pueden proteger todas las aplicaciones web públicas contra ataques y vulnerabilidades conocidas.
7. Restringir el acceso a los datos de los titulares de tarjetas previa justificación de la necesidad de acceso.	Cloudflare puede aplicar controles de acceso granulares con privilegios mínimos, independientemente de dónde se encuentren los usuarios o se almacenen los datos.
8. Identificar a los usuarios y autenticar el acceso a los componentes del sistema.	Cloudflare puede aplicar políticas basadas en la identidad y comprobaciones de la postura de seguridad (p. ej. si se ha utilizado la autenticación multifactor) para cualquier tráfico que pase por su red global.
10. Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de los titulares de tarjetas.	Cloudflare proporciona registros de auditoría granulares en todos los productos de su plataforma y se integra con la mayoría de los principales SIEM.
11. Probar la seguridad de los sistemas y redes con regularidad.	Cloudflare ofrece un servicio de detección de intrusos y pruebas de políticas de acceso limitado, además de registros detallados para todos sus productos principales.

*Cloudflare no ofrece soporte en cuanto a los requisitos 9 y 12 de la versión PCI DSS 4.0, que se refieren a la seguridad física y la estructura organizativa.

Resumen: Cloudflare te ayuda a cumplir los requisitos normativos de PCI. Confía en nosotros.

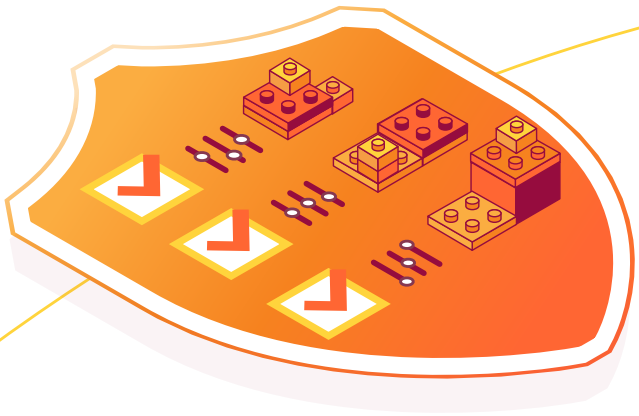
Cloudflare cumple la normativa PCI y tiene funciones que ayudan a los clientes a abordar por sí mismos los requisitos de conformidad, independientemente de cómo sea su infraestructura.

De hecho, el uso de las soluciones de Cloudflare puede reducir un 65 %[3] el posible riesgo de una filtración de datos, un 24%[4] las primas anuales de los seguros cibernéticos y un 59%[4] el tiempo dedicado a gestionar sistemas y procesos.

Nuestros clientes exigen contractualmente a Stax que cumpla unas normas de conformidad muy específicas. Este requisito nos llevó a aplicar controles de seguridad como Zero Trust en toda nuestra infraestructura [...] Cloudflare hizo exactamente lo que necesitábamos. Protegió nuestros puntos finales y nuestra seguridad". [5]

Troy Ridgewell
Responsable de seguridad, Stax

STAX



Descubre las soluciones de conformidad de datos de Cloudflare hoy mismo. Habla con nuestros expertos para empezar.

Referencias

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. Informe de IBM "Cost of Breach 2022"
4. Encuesta de TechValidate a clientes de servicios para aplicaciones de Cloudflare, 2023
5. https://www.cloudflare.com/es-es/case-studies/stax/

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-5776.09ABR2024