PCI DSS v4.0

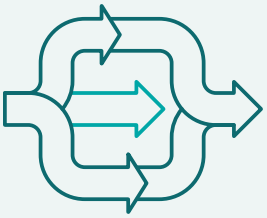
¿Qué es el Estándar de Seguridad de Datos PCI?

El Estándar de Seguridad de Datos PCI (PCI DSS) es un estándar global que proporciona una base técnica y operativa de requisitos designados para proteger los datos de pago. PCI DSS v4.0 es la siguiente evolución del estándar.

Metas de PCI DSS v4.0

Continuar Satisfaciendo las Necesidades de Seguridad de la Industria de Pagos

Promover la Seguridad como Proceso Continuo



Añadir Flexibilidad a las Diferentes Metodologías

Reforzar los Métodos de Validación

Desarrollado con la Colaboración de la Industria Global

El desarrollo de PCI DSS v4.0 fue motivado por la retroalimentación de la industria. Esta versión amplía la protección de los datos de pago con nuevos controles para hacer frente a sofisticados ciberataques.

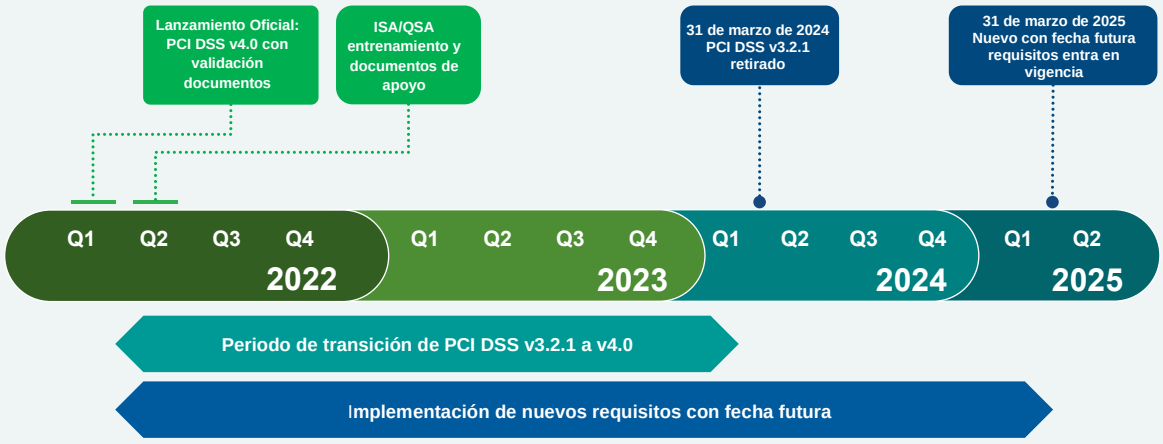
3
Solicitud de Comentarios (RFCs) Sobre el Contenido del Borrador

6,000+
Elementos de Comentarios Recibido

200+
Compañías Proporcionaron Comentarios

Calendario de Implementación

PCI DSS v3.2.1 permanecerá activo durante dos años después de la publicación de la v4.0. Esto proporciona a las organizaciones tiempo para familiarizarse con la nueva versión, y planificar e implementar los cambios necesarios.



¿Qué hay de Nuevo en el PCI DSS v4.0?

Se han incorporado muchos cambios en la última versión del Estándar. A continuación encontrará ejemplos de algunos de esos cambios. Para obtener una visión completa, consulte el Resumen de Cambios de PCI DSS v3.2.1 a v4.0, que se encuentra en la **Biblioteca de Documentos PCI SSC**.

Continuar satisfaciendo las necesidades de seguridad de la industria de pagos.

Por qué es importante: Las prácticas de seguridad deben evolucionar a medida que cambian las amenazas.

Ejemplos:

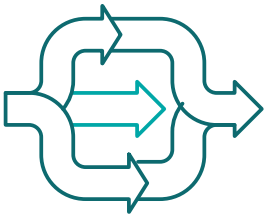
- Requisitos ampliados de la autenticación multifactorial.
- Requisitos de contraseña actualizados.
- Nuevos requisitos para el comercio electrónico y el phishing para hacer frente a las amenazas continuas.

Promover la seguridad como un proceso continuo.

Por qué es importante: Los criminales nunca duermen. La seguridad continua es crucial para proteger los datos de pago.

Ejemplos:

- Roles y responsabilidades claramente asignados en cada uno de los requisitos.
- Se ha añadido una guía para ayudar a las personas a comprender mejor cómo implementar y mantener la seguridad.



Aumentar la flexibilidad de las organizaciones que utilizan diferentes métodos para alcanzar los objetivos de seguridad.

Por qué es importante: Una mayor flexibilidad permite más opciones para lograr el objetivo de un requisito y apoya la innovación de la tecnología de pagos.

Ejemplos:

- Asignación de cuentas de grupos, compartidas y genéricas.
- Los análisis de riesgos específico permiten a las organizaciones establecer frecuencias para realizar ciertas actividades.
- El enfoque personalizado, un nuevo método para implementar y validar los requisitos PCI DSS, brinda otra opción a las organizaciones que utilizan métodos innovadores para lograr los objetivos de seguridad.

Reforzar los métodos y procedimientos de validación.

Por qué es importante: Las opciones claras de validación y la presentación de informes apoyan la transparencia y la granularidad.

Ejemplo:

- Una mayor alineación entre la información reportada en el Informe de Cumplimiento o el Cuestionario de Autoevaluación y la información resumida en la Atestación de Cumplimiento.

Suscríbase al **PCI Perspectives Blog**