PCI DSS

ESTÁNDARES DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETAS DE PAGO

senhasegura

1. INTRODUCCIÓN

1.1 Contexto

Las filtraciones de datos son una amenaza constante en sistemas de información de diversas industrias. Los sistemas de procesamiento de pagos con tarjetas son objetivos frecuentes de los atacantes, generando pérdidas financieras y afectando la confianza de los clientes.

El acceso privilegiado en la infraestructura tecnológica es crítico. Las credenciales de alto privilegio permiten modificar sistemas, lo que puede resultar en:

- Violaciones de conformidad con sanciones severas.
- Pérdida de confianza por incidentes de seguridad.

Para mitigar estos riesgos, en 2006 se creó el Payment Card Industry Security Standards Council (PCI SSC). Este consejo desarrolló el estándar PCI DSS, con el objetivo de proteger los datos de los titulares de tarjetas y garantizar medidas globales de seguridad.

El cumplimiento de PCI DSS es obligatorio para cualquier organización que almacene, procese o transmita datos de titulares de tarjetas. La gestión de acceso privilegiado (PAM) es fundamental para cumplir con este estándar, permitiendo visibilidad y control de las acciones administrativas. Soluciones como senhasegura son clave para garantizar el cumplimiento.

1.2 Objetivo

Este documento presenta los objetivos y requisitos del PCI DSS, destacando:

- La importancia de las credenciales privilegiadas.
- La relación entre la gestión de acceso privilegiado y PCI DSS.
- Cómo senhasegura ayuda a cumplir con estos requisitos.

2. CREDENCIALES PRIVILEGIADAS

Las credenciales privilegiadas son aquellas que permiten realizar acciones sin restricciones en los sistemas. Algunas de las más comunes incluyen:

1. Cuentas de Administrador Local: Usadas por el equipo de TI para mantenimiento.

2. Cuentas de Usuario Privilegiado: Pueden ser personales o impersonales, requieren especial atención.

3. Cuentas de Administrador de Dominio: Tienen control total sobre el dominio.

4. Cuentas de Emergencia: Permiten acceso en situaciones críticas.

5. Cuentas de Servicio: Usadas por aplicaciones para interactuar con otros sistemas.

6. Cuentas de Aplicación: Permiten acceso a bases de datos y aplicaciones.

Estadísticas: Según Verizon, el 22% de las filtraciones de datos analizadas involucraron credenciales robadas, lo que resalta la importancia de gestionar adecuadamente estas credenciales.

Tipos de credenciales privilegiadas

3. ESTÁNDAR PCI DSS

El PCI DSS se ha convertido en el marco práctico de controles de seguridad para proteger datos de tarjetas de pago y sus titulares. Además, su adopción se ha extendido para proteger otros datos sensibles, como información de identificación personal (PII), propiedad intelectual y datos de consumidores.

3.1 Requisitos de Cumplimiento del PCI DSS

El estándar PCI DSS consta de 12 requisitos agrupados en seis objetivos de control, que abarcan la gestión de seguridad, políticas, procedimientos, arquitectura de red y desarrollo de software para proteger los datos de tarjetas de pago. Este estándar incluye más de 200 controles individuales, enfocados en la confidencialidad de los datos. Todo comerciante o proveedor de servicios que almacene, procese o transmita datos de tarjetas de pago debe cumplir completamente con los controles aplicables a su entorno.

Los seis objetivos de control del PCI DSS son:

1. **Establecer y mantener la seguridad de redes y sistemas.**
2. **Proteger los datos del titular de la tarjeta.**
3. **Gestionar vulnerabilidades de manera continua.**
4. **Implementar controles de acceso estrictos.**
5. **Supervisar y probar redes regularmente.**
6. **Mantener una política sólida de seguridad de la información.**

Objetivo de Control	Requisito
Establecer y mantener la seguridad de redes y sistemas	- Instalar y mantener un firewall para proteger datos de tarjetas de crédito.
	- No utilizar contraseñas predeterminadas ni configuraciones de seguridad estándar en los sistemas.
Proteger los datos del titular de la tarjeta	- Proteger los datos almacenados de las tarjetas de crédito.
	- Usar cifrado para la transmisión de datos de tarjetas de crédito.
Gestionar vulnerabilidades de manera continua	- Utilizar programas antivirus regularmente.
	- Desarrollar y mantener sistemas y aplicaciones seguras.
Implementar controles estrictos de acceso	- Restringir el acceso a los datos de tarjetas de crédito solo a personas y roles necesarios.
	- Asignar un ID único a cada usuario de la red y sistemas.
	- Restringir el acceso físico a los datos de tarjetas de crédito.
Supervisar y probar las redes regularmente	- Rastrear y monitorear todos los accesos a la red y a los datos de tarjetas de crédito.
	- Probar regularmente la seguridad de los sistemas y procesos.
Mantener una política sólida de seguridad de la información	- Establecer y mantener una política que aborde la seguridad de la información.

Requisitos y Objetivos de Control del Estándar PCI DSS

3.2. Niveles de Conformidad del PCI DSS

Las organizaciones se clasifican en 4 niveles según su volumen de transacciones:

Nivel	Transacciones Anuales	Requisitos
Nivel 1	Más de 6 millones	- Evaluación anual de seguridad de datos.
		- Verificación trimestral de vulnerabilidades de red.
Nivel 2	Entre 1 y 6 millones	- Cuestionario de autoevaluación anual.
		- Verificación trimestral de vulnerabilidades de red.
Nivel 3	Entre 20 mil y 1 millón	- Cuestionario de autoevaluación anual.
		- Verificación trimestral de vulnerabilidades de red.
Nivel 4	Hasta 20,000	- Cuestionario de autoevaluación anual.
		- Verificación trimestral de vulnerabilidades de red.

Niveles de Cumplimiento del Estándar PCI DSS

3.3. Penalidades por Incumplimiento:

- Multas de hasta $500,000 por incidentes de fuga de datos.
- Daños reputacionales y pérdida de confianza de clientes.
- Normativas adicionales como GDPR que pueden imponer sanciones severas.

4. Soluciones PAM para Cumplimiento con PCI DSS

La Gestión de Acceso Privilegiado (PAM) es esencial para proteger credenciales privilegiadas, reducir riesgos y cumplir con estándares como PCI DSS. Las credenciales con altos privilegios son usadas tanto por empleados como por terceros, lo que aumenta los riesgos de fugas y amenazas internas.

Beneficios clave de PAM para datos de tarjetas de pago:

1. **Romper el ciclo de ataque:** Detiene a los atacantes al limitar su capacidad de moverse y escalar privilegios.
2. **Mitigar amenazas internas:** Cerca del 30% de las filtraciones involucran actores internos.
3. **Monitorear acciones privilegiadas:** Facilita auditorías y la detección rápida de incidentes.
4. **Eliminar contraseñas embebidas:** Evita que credenciales en scripts sean usadas por atacantes o accesibles por error.

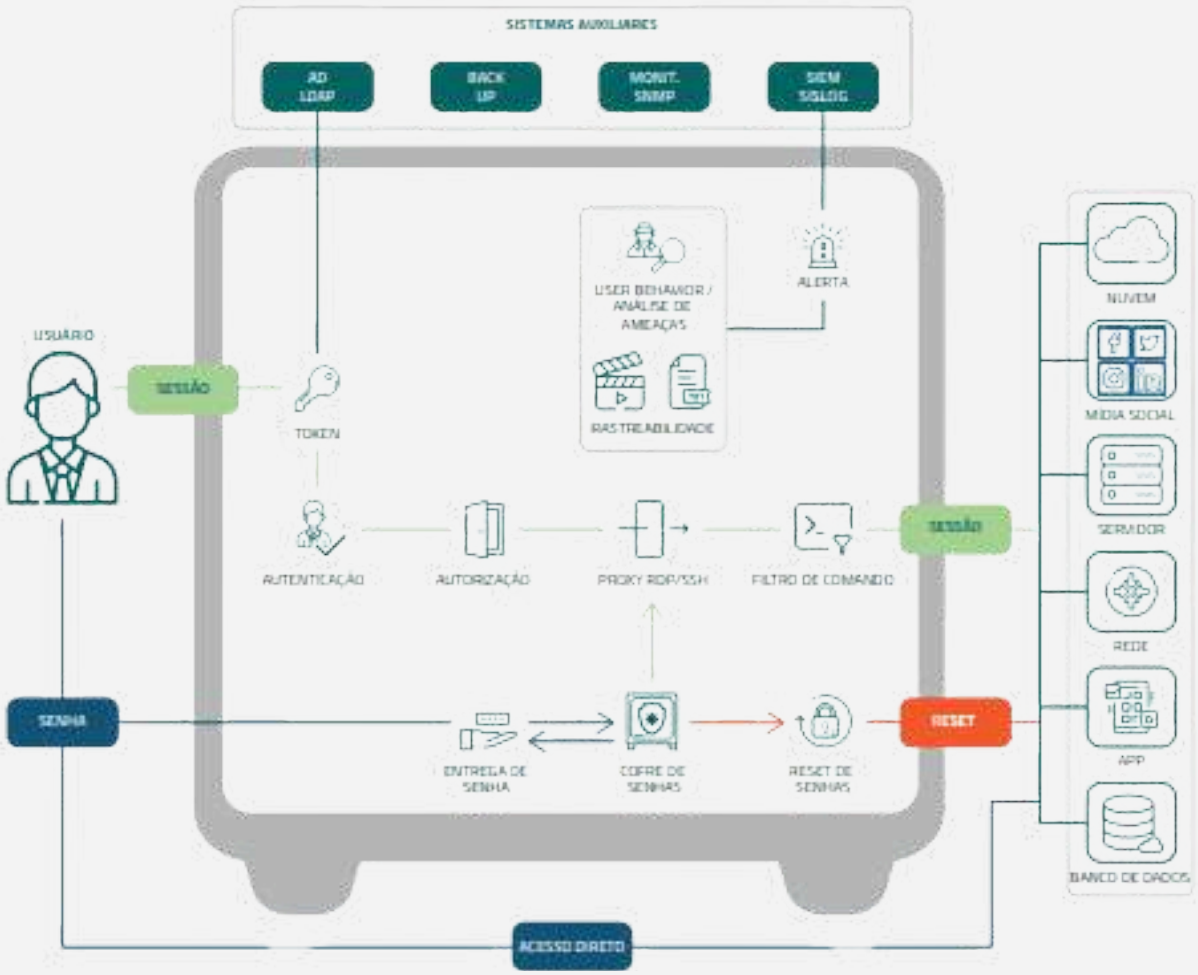
Soluciones como senhasegura simplifican el cumplimiento con PCI DSS al gestionar el acceso privilegiado de forma segura y eficiente.

5. Senhasegura: Gestión Segura de Credenciales

Senhasegura es una solución de software y hardware diseñada para almacenar, gestionar y monitorear credenciales privilegiadas, como contraseñas, claves SSH y certificados digitales, en un entorno seguro. Además, registra todas las sesiones remotas para auditorías y genera alertas en tiempo real para identificar acciones indebidas.

Contribución de senhasegura al cumplimiento de PCI DSS:

- **Requisito 2:** Elimina contraseñas predeterminadas y restringe protocolos inseguros, como SSH o SSL/TLS.



Flujo de Gestión de Acceso Privilegiado a través de senhasegura

senhasegura®

- **Requisito 6:** Gestiona credenciales y segrega roles en desarrollo, prueba y producción.
- **Requisito 7:** Implementa el principio de mínimo privilegio mediante accesos granulares, workflows de aprobación y accesos emergentes.
- **Requisito 8:** Garantiza autenticación única, soporte de 2FA y manejo de credenciales compartidas en entornos híbridos.
- **Requisito 10:** Registra y rastrea accesos privilegiados, ofreciendo logs inviolables y visibilidad total de las acciones.

5.1 Beneficios de Implementar Senhasegura

1.Reducción de Costos: Minimiza los gastos de auditoría PCI DSS con control centralizado de accesos.

2.Incremento de Seguridad: Prevención y mitigación de riesgos relacionados con usuarios privilegiados.

3.Implementación Rápida: Despliegue sencillo e integración ágil con infraestructuras existentes.

6. Conclusión

La protección de datos sensibles y la gestión de acceso privilegiado son fundamentales para cumplir con PCI DSS. Con soluciones como senhasegura, las organizaciones pueden fortalecer su seguridad y garantizar la conformidad con los estándares más exigentes de la industria.

Cumplir con PCI DSS nunca fue tan fácil ni tan seguro como con Senhasegura

senhasegura®

¡Eleva tu seguridad hoy!

Contáctanos y descubre
cómo podemos ayudarte

www.inntech.com.mx/contacto

+52 (55) 5488 7630