TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

Fundamentos de Seguridad de la Informacion

Introducción

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS, por sus siglas en inglés) es un conjunto de requisitos de seguridad establecidos para proteger la información de las tarjetas de pago. Su objetivo principal es reducir el fraude y garantizar la seguridad en las transacciones con tarjetas de crédito y débito.

El cumplimiento de PCI DSS es fundamental para garantizar la seguridad en la industria de tarjetas de pago. Implementar y mantener estos estándares protege tanto a las empresas como a los consumidores contra amenazas cibernéticas y fraudes financieros.

Origenes y organizaciones involucradas

El PCI DSS fue desarrollado por el Consejo de Normas de Seguridad PCI (PCI SSC), fundado en 2006 por las principales marcas de tarjetas de pago: Visa, MasterCard, American Express, Discover y JCB.



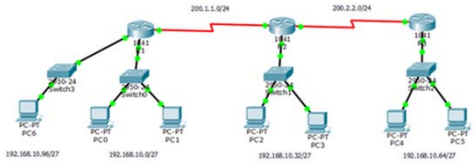
Requisitos

El estándar se compone de 12 requisitos fundamentales agrupados en 6 objetivos principales:

Objetivos	Requisitos
1.- Construir y mantener una red segura	Instalar y mantener una configuración segura de firewalls. No utilizar contraseñas y configuraciones predeterminadas.
2. Proteger los datos del titular de la tarjeta	Proteger los datos almacenados. Cifrar la transmisión de datos del titular de la tarjeta en redes abiertas y públicas.
3.- Mantener un programa de gestión de vulnerabilidades	Usar y actualizar software antivirus regularmente. Desarrollar y mantener sistemas y aplicaciones seguras.
4 .- Implementar medidas estrictas de control de acceso	Restringir el acceso a los datos según la necesidad de conocer. Asignar un ID único a cada persona con acceso a los datos. Restringir el acceso físico a los datos del titular de la tarjeta.
Monitorear y probar redes regularmente:	Rastrear y monitorear el acceso a los datos del titular de la tarjeta. Probar regularmente los sistemas y procesos de seguridad.
Mantener una política de seguridad de la información:	Mantener una política de seguridad que se aplique a todos los empleados.

Requisitos

Los **datos del titular de la tarjeta** deben cifrarse en tránsito y, cuando sea necesario, también en reposo para evitar el acceso no autorizado.	Solo **almacene la cantidad mínima** de datos necesarios para el negocio y durante el menor tiempo posible.	**Segmentar la red** para separar los sistemas de datos de tarjetas de otros sistemas, reduciendo así el alcance y el riesgo de comprometer los datos.	Utilizar **métodos de autenticación robustos** y asegurar que los accesos se gestionen de manera controlada y monitoreada.
Cifrado y protección de datos	Minimización de datos	Segmentación de la red	Autenticación de la fuente



Inacap

Beneficios

- Protección contra brechas de seguridad y fraude.
- Mejora de la confianza del cliente.
- Reducción de responsabilidades legales y financieras en caso de incidentes.
- Cumplimiento con regulaciones internacionales y locales.





Inacap

¿Quiénes deben cumplir con PCI DSS?

- Comercios minoristas y en línea.
- Procesadores de pago.
- Instituciones financieras.
- Proveedores de servicios que manejan datos de tarjetas.







nacap

Niveles de cumplimiento

Nivel 1: Más de 6 millones de transacciones.
Nivel 2: De 1 a 6 millones de transacciones.
Nivel 3: De 20,000 a 1 millón de transacciones.
Nivel 4: Menos de 20,000 transacciones.

nacap

Quién regula en Chile las TC /TD

En Chile, la Comisión para el Mercado Financiero (CMF) y la Superintendencia de Bancos e Instituciones Financieras (SBIF) son las instituciones que regulan y fiscalizan las tarjetas de crédito.