Payment Card Industry Data Security Standard (PCI DSS)

Para personas que:

- Procesan datos.
- Almacenan datos.
- Transmiten datos.
  Para poder:
- Asegurar datos.
- Evitar fraudes.

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago fue desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes (denominado PCI SSC - Payment Card Industry Security Standards Council). Funciona como una guía para ayudar a las organizaciones de tarjetahabientes (o titulares de tarjeta), con aspectos que involucran tarjetas de pago, débito y crédito.

Las compañías deben cumplir con el estándar o arriesgan:

- Pérdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de franquicias).
- Enfrentar auditorías rigurosas
- Pagos de multas.

Y deben validar el cumplimiento del estándar de forma periódica, validación realizada por **Qualified Security Assessor (QSAs)**.
Solo a las compañías que procesan menos de 80,000 transacciones por año se les permite ejecutar una autoevaluación utilizando un cuestionario provisto por el Consejo.

Requisitos:

12 requisitos en 6 secciones relacionadas lógicamente, llamadas "objetivos de control."

Los objetivos de control y sus requisitos son los siguientes:

1. **Desarrollar** y **mantener** una red segura:
    1. *Requisito 1:* Instalar y mantener una configuración de **firewalls** para proteger los datos de los propietarios de tarjetas.
    2. *Requisito 2:* **No** usar contraseñas del sistema y otros parámetros de seguridad **predeterminados** provistos por los proveedores.
2. **Proteger** los datos de los propietarios de tarjetas:
    1. *Requisito 3:* Proteger los datos almacenados de los propietarios de tarjetas.

    2. *Requisito 4:* **Cifrar** los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
3. Mantener un Programa de **Gestión** de **Vulnerabilidades**:
    1. *Requisito 5:* Usar y actualizar regularmente un software **antivirus**.
    2. *Requisito 6:* Desarrollar y mantener sistemas y **aplicaciones seguras**.
4. Implementar Medidas sólidas de **control de acceso**:
    1. *Requisito 7:* **Restringir** el **acceso lógico** a los datos tomando como base la necesidad del funcionario de conocer la información.
    2. *Requisito 8:* Asignar una **identificación única** a cada persona que tenga acceso a un computador.
    3. *Requisito 9:* **Restringir** el **acceso físico** a los datos de los propietarios de tarjetas.
5. **Monitorizar** y **probar** regularmente las redes:
    1. *Requisito 10:* **Rastrear** y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
    2. *Requisito 11:* Probar regularmente los **sistemas y procesos** de seguridad.
6. Mantener una **Política** de Seguridad de la Información:
    1. *Requisito 12:* Mantener una política que contemple la seguridad de la información