RESUMEN DE NORMA · CERT.GT

PCI DSS

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Comercios, procesadores, bancos y proveedores que tocan datos de tarjetas.

PCI DSS es el estándar de seguridad para quien almacena, procesa o transmite datos de tarjetas de pago. No es una ley: lo exigen las marcas de tarjetas a través de los bancos adquirentes, por contrato. La versión vigente es la 4.0.1.

Lo esencial

- Aplica si aceptas tarjetas, aunque sea con un solo datáfono o un botón de pago en tu sitio.
- La versión 3.2.1 se retiró el 31 de marzo de 2024. Los requisitos nuevos de la versión 4 son obligatorios desde el 31 de marzo de 2025.
- La mejor forma de cumplir es reducir el alcance: mientras menos sistemas toquen datos de tarjeta, menos hay que proteger y auditar.
- Nunca guardes el código de seguridad (CVV), el PIN ni la banda magnética después de la autorización, ni siquiera cifrados.

Los 12 requisitos

1	Instalar y mantener controles de seguridad de red.
2	Aplicar configuraciones seguras a todos los componentes del sistema.
3	Proteger los datos de cuenta almacenados.
4	Proteger los datos del titular con criptografía fuerte al transmitirlos por redes públicas.
5	Proteger todos los sistemas y redes contra software malicioso.
6	Desarrollar y mantener sistemas y software seguros.
7	Restringir el acceso a los datos según la necesidad de conocerlos.
8	Identificar a los usuarios y autenticar el acceso.
9	Restringir el acceso físico a los datos del titular.
10	Registrar y monitorear todo acceso a los sistemas y a los datos.
11	Probar con regularidad la seguridad de sistemas y redes.
12	Respaldar la seguridad de la información con políticas y programas de la organización.

Lo nuevo en la versión 4

- Verificación en dos pasos para todo acceso al entorno de datos de tarjeta, no sólo para administradores.
- Contraseñas de al menos 12 caracteres.
- Control de los scripts que cargan las páginas de pago y detección de cambios no autorizados en ellas.
- Protección técnica contra phishing y revisión automatizada de registros.
- Opción de “enfoque personalizado”: cumplir el objetivo de un requisito con un control distinto, si se demuestra que funciona.
- Análisis de riesgo específico para definir la frecuencia de varias actividades periódicas.

Cómo se valida

- El nivel del comercio depende del número de transacciones al año y lo define cada marca; tu banco adquirente te dice cuál te corresponde.
- Los comercios pequeños llenan un cuestionario de autoevaluación (SAQ); hay varios tipos según cómo aceptes tarjetas.
- Los niveles más altos requieren una auditoría en sitio por un evaluador calificado (QSA) y un informe de cumplimiento (ROC).
- Si tienes sistemas expuestos a internet, se exigen escaneos trimestrales por un proveedor aprobado (ASV).

Cómo reducir el alcance

- Usa una pasarela o página de pago alojada por el procesador: así los datos de tarjeta no pasan por tus servidores.
- Usa terminales con cifrado punto a punto validado (P2PE).
- Reemplaza el número de tarjeta por un token si necesitas hacer cobros recurrentes.
- Separa en la red los sistemas que tocan tarjetas del resto de la empresa.

Errores frecuentes

- Guardar números de tarjeta en hojas de cálculo, correos o grabaciones de llamadas.
- Creer que tercerizar el pago elimina toda la responsabilidad: sigues respondiendo por tu parte del proceso.
- Cumplir una vez al año para la auditoría y no mantener los controles el resto del tiempo.

Texto oficial

PCI DSS v4.0.1, del PCI Security Standards Council, gratuito en pcisecuritystandards.org.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Resumen elaborado por cert.gt con fines educativos; no es el texto oficial de la norma ni sustituye asesoría legal o de cumplimiento. No es un documento de una entidad gubernamental. Puedes copiarlo y adaptarlo citando la fuente (CC BY 4.0).