



Conformidad con PCI DSS

(Payment Card Industry Data Security Standards)

Normas de seguridad de PCI

Las normas de seguridad de PCI han sido desarrolladas para fomentar y mejorar la seguridad de los datos de los titulares de tarjetas y facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Desde su inicio en 2006, han sido desarrolladas por el **PCI Security Standards Council** y hacen referencia a varios ámbitos diferentes:



PCI DSS, PA-DSS, PCI PTS

Cada una de las tres normas definidas por PCI se centra en un ámbito específico.

Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las **PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago** (comerciantes, instituciones financieras, entidades adquirentes, entidades emisoras, proveedores de servicios...) y, en general, toda organización que almacene, procese o transmita datos de titulares de tarjetas.

Por su parte, las **PA-DSS se aplican a proveedores de software** y demás que desarrollan aplicaciones de pago que almacenan, procesan o transmiten datos de titulares de tarjetas, siempre que dichas aplicaciones se vendan, distribuyan u otorguen bajo licencia a terceros.

Finalmente, **PCI PTS aplica a los dispositivos de pago**, definiendo los requisitos para su fabricación.

Requisitos y obligaciones respecto a PCI DSS

De las tres normas, PCI DSS es la que más repercusión ha tenido. Todas las organizaciones afectadas por PCI DSS deben **cumplir, validar y reportar el cumplimiento de la norma**. No obstante, las formas de validar y reportar el cumplimiento varían según la marca de tarjetas involucradas, principalmente basándose en el tipo de organización o el volumen de transacciones.

Así por ejemplo, de las cinco marcas de tarjetas, **VISA y Mastercard definen cuatro niveles para comercios**:

¿Quiénes forman el PCI SSC?

El PCI Security Standards Council es un foro mundial abierto, establecido en 2006, que se encarga de la formulación, gestión, educación y conocimiento de las normas de seguridad de la industria de tarjetas de pago.



Los cinco miembros fundadores (*American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc.*) acordaron incorporar PCI DSS como los requisitos técnicos de cada uno de sus programas de cumplimiento en materia de seguridad. Además, reconocen que los **Evaluadores de Seguridad Certificados (QSA)** y los **Proveedores Aprobados de Escaneo (ASV)** certificados por el PCI SSC son los únicos habilitados para validar el cumplimiento con PCI DSS.

De este modo, con las normas de PCI se unifican los requisitos propios de cada una de las marcas de tarjetas, simplificando así el proceso de cumplimiento con cada una de ellas y facilitando su adopción. **En caso de no cumplir con la norma**, las marcas de tarjeta con quienes se opere pueden imponer sanciones o multas, llegando, incluso, a la denegación del servicio de utilización de sus tarjetas.

Resumen de condiciones	Obligaciones
1 <ul style="list-style-type: none"> • Si procesan más de seis millones de transacciones anuales, con independencia del canal • Si se hubiera comprometido la información de tarjetas • Si fuera considerado de nivel 1 por cualquier miembro de PCI 	<ul style="list-style-type: none"> • Auditoría anual por un QSA • Escaneo de red trimestral con un ASV
2 <ul style="list-style-type: none"> • Si procesan entre uno y seis millones de transacciones anuales, con independencia del canal 	<ul style="list-style-type: none"> • Cuestionario de autoevaluación anual
3 <ul style="list-style-type: none"> • Si procesan entre 20.000 y un millón de transacciones anuales a través de Internet 	<ul style="list-style-type: none"> • Escaneo de red trimestral con un ASV
4 <ul style="list-style-type: none"> • El resto* 	

* En el caso de Visa, los requisitos para el nivel 4 son sólo recomendaciones

En el caso de **proveedores de servicios**, las condiciones son similares, si bien sólo diferencian dos niveles:

Resumen de condiciones	Obligaciones
1 <ul style="list-style-type: none"> • Si almacenan, procesan o transmiten más de 300.000 transacciones anuales, con independencia del canal • Si se hubiera comprometido la información de tarjetas 	<ul style="list-style-type: none"> • Auditoría anual por un QSA • Escaneo trimestral con un ASV
2 <ul style="list-style-type: none"> • Si almacenan, procesan o transmiten menos de 300.000 transacciones anuales, con independencia del canal 	<ul style="list-style-type: none"> • Cuestionario de autoevaluación anual • Escaneo de red trimestral (con un ASV en el caso de Visa)

Como puede verse, en los niveles menos exigentes se acepta la revisión mediante cuestionarios de autoevaluación (SAQ), que pueden ser respondidos por los propios afectados. No obstante, es altamente recomendable contar con el asesoramiento o experiencia de auditores QSA certificados.

Servicios profesionales de SIA sobre PCI

En SIA, con más de 20 años como proveedores de servicios de seguridad, **contamos con la certificación QSA** emitida por PCI SSC. Esta nos permite acreditar el cumplimiento de la norma conforme a los requisitos establecidos por las marcas de tarjetas, así como asistir a la hora de cumplimentar los cuestionarios de autoevaluación. Además, gracias a acuerdos de colaboración con compañías **ASV**, complementamos nuestros servicios con la realización de los escaneos de red trimestrales conforme a la norma.

SIA cuenta con un amplio bagaje en el ámbito de la seguridad de la información y dispone de un gran equipo de profesionales de muy alta capacitación y experiencia, en disposición de certificaciones como CISA, CISM, CGEIT, CRISC, LA 27001, CISSP, o CEH, entre otras.

El valor de SIA como aliado en el cumplimiento de PCI no sólo se queda en la auditoría. Nuestra condición de proveedores de soluciones integrales nos permite ofrecer **soluciones óptimas para el cumplimiento de PCI** en cada uno de sus doce requisitos, unificándolo con el cumplimiento de otros marcos similares, como los derivados de la LOPD, los SGSI, ITIL, COBIT, ... o las propias políticas internas de cada compañía.

Requisitos de PCI DSS

A continuación, se incluye una descripción general de los 12 requisitos de las PCI DSS:

Desarrollar y mantener una red segura	1. Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.
Proteger los datos del titular de la tarjeta	2. No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Mantener un programa de administración de vulnerabilidad	3. Proteja los datos del titular de la tarjeta que fueron almacenados.
Implementar medidas sólidas de acceso	4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Supervisar y evaluar las redes con regularidad	5. Utilice y actualice regularmente el software o los programas antivirus.
Mantener una política de seguridad de información	6. Desarrolle y mantenga sistemas y aplicaciones seguras.
	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.
	8. Asignar una ID exclusiva a cada persona que tenga acceso por computadora.
	9. Restringir el acceso físico a los datos del titular de la tarjeta.
	10. Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas.
	11. Pruebe con regularidad los sistemas y procesos de seguridad.
	12. Mantenga una política que aborde la seguridad de la información para todo el personal.

Enfoque metodológico

SIA fomenta el cumplimiento de PCI DSS con un enfoque orientado a la mejora continua de la seguridad de los sistemas afectados, orientando a sus clientes a mantener y aumentar la seguridad de forma global.

Habitualmente, nuestros servicios sobre PCI se desarrollan en cuatro fases, que tienen como principales objetivos delimitar el entorno afectado, identificar los puntos de no conformidad con la norma y orientar en las acciones que deban tomarse para subsanarlos, hasta la emisión del informe final.



Debido al coste que supone la implementación de los requisitos PCI DSS, en la primera fase del proyecto cobra especial importancia la delimitación del alcance y la identificación de los componentes afectados. En muchas ocasiones, **es posible reducir el coste y esfuerzo** utilizando una adecuada segmentación de red, eliminando datos innecesarios, aislando sistemas, etc. Es por ello que SIA recomienda dedicar el esfuerzo necesario en esta primera fase con objeto de simplificar el posterior proceso de cumplimiento.

Durante la fase de análisis, utilizamos los **procedimientos de prueba y criterios de evaluación definidos por PCI**. Sólo de esta forma es posible garantizar el cumplimiento de los requisitos frente a quienes después exigirán los informes de auditoría (entidades adquirentes, comercios o las propias compañías de tarjetas). Identificamos no sólo los puntos de no conformidad, sino también las oportunidades de mejora y recomendaciones para el cumplimiento de PCI DSS.

Transcurrido un plazo razonable para que el auditado pueda resolver las no conformidades, se prepara el **Informe de Cumplimiento** y la **Declaración de Cumplimiento**. En este punto, será fundamental haber identificado los requisitos de reporte y los formatos con lo que habrá que hacerlo, según quién sea el solicitante y el nivel exigido.



Grupo SIA, a partir de la experiencia en el ámbito de la seguridad de la información puede ayudar a sus clientes en el cumplimiento de normas de seguridad y aumento y mejora de la seguridad de la información a través de los otros servicios, como son:

- Implantación de SGSI y análisis de riesgos.
- Planes de Continuidad de Negocio.
- Auditoría y adecuación normativa.
- Adecuación a las buenas prácticas de ITIL.
- Marco normativo de seguridad de la información.
- Planes de formación y concienciación.
- Governance, Risk and Compliance.
- Segmentación red.
- Seguridad perimetral.
- Monitorización eventos, recogida de logs y correlación.

Grupo SIA, proveedor global de seguridad, tiene las siguientes certificaciones que avalan la madurez de los servicios que presta:

- Qualified Security Assessor – PCI DSS
- Gestión de la Calidad – UNE-EN-ISO 9001:2000
- Gestión de Seguridad de la Información – UNE-ISO/IEC 27001
- Gestión de Servicios IT – UNE-ISO/IEC 20000
- Gestión de Medio Ambiente – ISO 14001:2004
- Gestión de la Innovación – UNE 166002:2006
- Calidad de Software (SPICE Nivel 2) – ISO 15504



www.sia.es

Avda. de Europa, 2 · Alcor Plaza · Edificio B
Parque Oeste Alcorcón · 28922 Alcorcón
Tel: +34 902 480 580
Fax: +34 913 077 980

