Guia PCI DSS

ÍNDICE

1. PCI DSS
2. DATOS DE CUENTAS
3. PCI DSS Y PA DSS
4. WEBGRAFÍA

PCI-DSS

El estándar PCI-DSS (Payment Card Industry Data Security Standard) fue desarrollado por un comité denominado PCI SSC (Payment Card Industry Security Standards Council) y hace foco en las redes, sistemas y otros equipos que permiten procesar transacciones realizadas con tarjetas de pago (crédito y débito).

La PCI DSS se aplica en todas las empresas que participan en el procesamiento o almacenamiento de la información de las tarjetas de pago.

Estas pueden ser:

- Comerciantes
- Entidades Procesadoras
- Entidades emisoras

Las primeras versiones se remontan a Octubre de 2008, la última versión es la **v3.2.1 (Abril de 2018)**.

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción	Páginas
Octubre de 2008	1.2	Introducir la versión 1.2 de las PCI DSS (Normas de seguridad de datos de la industria de tarjetas de pago) como "requisitos de las PCI DSS y procedimientos de evaluación de seguridad" para eliminar la redundancia entre documentos e implementar cambios generales y específicos de los procedimientos de auditoría de seguridad de la versión 1.1 de las PCI DSS. Para obtener la información completa, consulte el Resumen de cambios de la Normas de seguridad de datos de la PCI de las PCI DSS, versión 1.1 a 1.2.	
Julio de 2009	1.2.1	Agregar la oración que se eliminó incorrectamente entre las PCI DSS versión 1.1 y 1.2.	5
		Corregir "then" por "than" en los procedimientos de prueba 6.3.7.a y 6.3.7.b.	32
		Eliminar la marca gris para las columnas "Implementado" y "No implementado" en el procedimiento de prueba 6.5.b.	33
		Para la Hoja de trabajo de controles de compensación - Ejemplo completo, corregir la redacción al principio de la página de modo que diga "Utilizar esta hoja de trabajo para definir los controles de compensación para cualquier requisito indicado como 'implementado' a través de los controles de compensación".	64
Octubre de 2010	2.0	Actualizar e implementar cambios de la versión 1.2.1. Consulte *PCI DSS: Resumen de cambios de la versión 1.2.1 a 2.0 de las PCI DSS.*	
Noviembre de 2013	3.0	Actualización de la versión 2.0. Consulte *PCI DSS: Resumen de cambios de la versión 2.0 a 3.0 de las PCI DSS.*	
Abril de 2015	3.1	Actualización de la PCI DSS, versión 3.0. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.0 a 3.1*	
Abril de 2016	3.2	Actualización de la PCI DSS, versión 3.1. Para obtener los detalles, consulte *PCI DSS - Resumen de cambios de la PCI DSS versión 3.1 a 3.2*	

Todas estas normas se desarrollaron para mejorar la seguridad de los datos del titular

Los puntos generales o requisitos de la DSS son los siguientes:

Desarrollar redes y sistemas seguros.

1. Configuración para proteger datos.
2. No usar valores predeterminados para contraseñas o parámetros de seguridad.

Proteger Datos del titular de la tarjeta.

3. Proteger datos de la tarjeta
4. Cifrar la transmisión de datos en redes públicas abiertas

Mantener programa administracion de vulnerabilidad.

5. Proteger los sistemas contra malware, actualizar programas o antivirus de forma regular.
6. Mantener sistemas y aplicaciones seguras.

Implementar medidas de control de acceso.

7. Restringir acceso a datos dependiendo de la necesidad de saber que tenga la empresa
8. Identificar / Autenticar el acceso a los componentes del sistema.
9. Restringir acceso físico a los datos del titular

Evaluar redes con regularidad.

10. Revisar todos los accesos a los recursos en red y a los datos.
11. Revisar de forma periódica los sistemas y procesos de la seguridad

Mantener una política de seguridad de la información.

12. Tener una política de seguridad que englobe a todo el personal

Normas de seguridad de datos de la PCI: descripción general de alto nivel

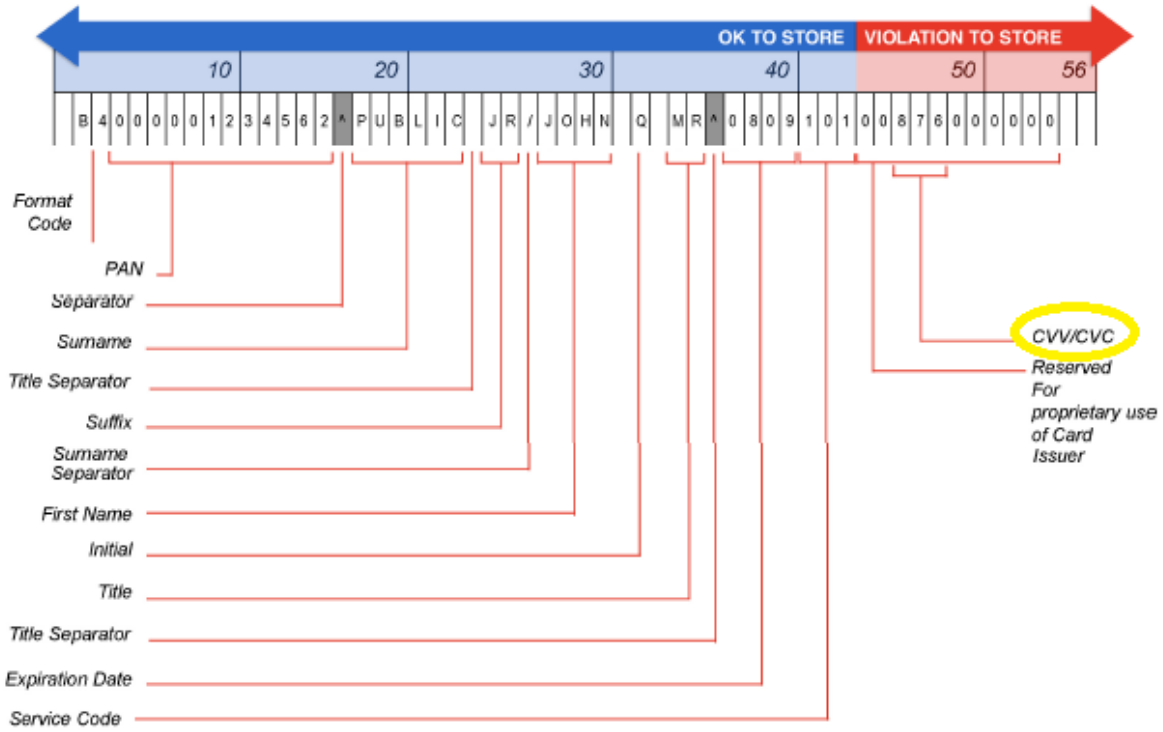
Desarrolle y mantenga redes y sistemas seguros.	**1.** Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. **2.** No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	**3.** Proteja los datos del titular de la tarjeta que fueron almacenados **4.** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	**5.** Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. **6.** Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	**7.** Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. **8.** Identificar y autenticar el acceso a los componentes del sistema. **9.** Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	**10.** Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta **11.** Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	**12.** Mantener una política que aborde la seguridad de la información para todo el personal

DATOS DE CUENTAS

Los datos de cuentas a proteger son los siguientes registros:

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

		Elemento de datos	Almacenamiento permitido	Datos almacenados ilegibles según el Requisito 3.4
Datos de cuentas	**Datos del titular de la tarjeta**	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN[5]	No	No se pueden almacenar según el Requisito 3.2



PCI DSS y PA-DSS

El estándar PA-DSS (Payment Application Data Security Standard o Estándar de Seguridad de Datos para Aplicaciones de Pago) tiene una estructura similar, pero se centra en las aplicaciones de pago con tarjetas.

Un **punto a tener en cuenta** es el siguiente:

"El uso de una aplicación que cumpla con las PA-DSS por sí sola no implica que una entidad cumpla con las PCI DSS, dado que esa aplicación se debe implementar en un entorno que cumpla con las PCI DSS y de acuerdo con la Guía de implementación de las PA-DSS proporcionada por el proveedor de la aplicación de pago."

Cumplir con el PA-DSS no significa cumplir con el PCI-DSS

Para que a las empresas nuevas les resulte "más fácil" el proceso de validación del cumplimiento de la normativa PCI, el Consejo PCI creó nueve formularios diferentes o cuestionarios de autoevaluación (SAQ) que subdividen los requisitos de la normativa PCI.

https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2.pdf

WEBGRAFÍA

https://www.owisam.org/index.php?title=Metodologia

https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2-1-ES-LA.PDF

https://es.pcisecuritystandards.org/minisite/env2/

https://www.browserling.com/tools/text-to-ascii

https://www.fpgenred.es/GNU-Linux/el_problema_del_final_de_lnea.html

https://es.pcisecuritystandards.org/minisite/env2/

https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-ii-cidcav2cvc2cvv2/

https://www.helpsystems.com/es/recursos/articulo/cumplimiento-pci-y-pa-dss-que-es-requisitos-latinoamerica-espana

https://www.pcihispano.com/que-es-pa-dss-pci-ssf-pci-s3-pci-secure-slc/

https://www.helpsystems.com/cta/download-pci-guide

https://www.pcisecuritystandards.org/documents/PA-DSS-v3_2-Program-Guide.pdf?agreement=true&time=1637084968478

https://stripe.com/es-us/guides/pci-compliance

https://www.ambito.com/negocios/criptomonedas/las-tambien-llegan-la-copa-libertadores-n5323958

https://www.telesemana.com/blog/2021/11/25/los-servicios-virtualizados-de-tencent-desembarcaron-en-america-latina-al-inaugurar-centro-de-datos-en-brasil/