Universidad Piloto de Colombia
UN ESPACIO PARA LA EVOLUCIÓN

ESTÁNDAR DE SEGURIDAD EN LA INDUSTRIA DE LAS TARJETAS DE PAGO - PCI DSS

Christian Camilo Vanegas Pacheco

Ingeniero Electrónico. Universidad Manuela Beltrán

Chr_van1@hotmail.com

Resumen

El estándar PCI-DSS plantea un conjunto mínimo de requisitos y procedimientos impuestos por la industria de las tarjetas de pago, que buscan asegurar la información confidencial de los tarjetahabientes, además de facilitar la adopción de medidas de seguridad utilizadas a nivel mundial.

Dicho estándar se aplica a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se destacan los comerciantes, las entidades emisoras y proveedoras de servicios, así como también las entidades que almacenan, procesan o transmiten datos de los titulares de las tarjetas.

Por lo tanto este documento busca presentar al lector de manera clara una visión general de los requisitos necesarios del estándar y de esta forma, poder comprender la importancia del uso de controles y la adopción de buenas prácticas de seguridad con el fin de mitigar los riesgos asociados al uso de las tarjetas de pago.

Palabras claves

PCI, estándar, cumplimiento, tarjetas de pago.

Abstract

PCI-DSS presents a minimum set of requirements and procedures imposed by the card industry to pay, which seek to secure confidential cardholder information and facilitates the adoption of security measures used worldwide.

This standard applies to all entities involved in the process of payment cards, including highlighting the merchants, issuers and service providers, as well as entities that store, process or transmit cardholder data of the cards.

Therefore this paper aims to present the reader with a clear overview of the requirements of the standard and thus to understand the importance of using controls and the adoption of good security practices to mitigate risks associated the use of payment cards

Keywords

PCI, standard, compliance, payment card.

Introducción

La necesidad de un estándar para proteger la información de los tarjetahabientes en la industria de las tarjetas de pago, se inició en el año 2001 con los programas de seguridad para proteger la información de los titulares de las mismas. De una parte *Visa's Cardholder Information Security Program* (CISP) y de otra *MasterCard's Site Data Protection* (SDP).

En el año 2003, el programa CISP se amplió de los procesadores y emisores de tarjetas, a los comerciantes de alto volumen y proveedores de servicios. Luego, en el año 2006, [1] las cinco principales marcas de la industria de las tarjetas de pago unieron sus esfuerzos con el fin de crear la norma PCI-DSS (*Payment Card Industry Data Security Standard*) y de esta forma unificar los estándares de cumplimiento para las organizaciones que procesan, almacenan o transmiten información de las tarjetas de pago.

A través de este documento no se pretende abordar el estándar PCI-DSS desde el punto de vista netamente técnico ni abrumar al lector con el análisis detallado de cada ítem de la norma, por el contrario se busca presentarlo de manera general, para que tenga una visión global que le servirá de referencia para poder aplicarlo en su organización.

Para la elaboración del mismo se consultaron diferentes referencias bibliográficas entre las que se destacan como fuente principal los documentos del *Security Standards Council* referentes al estándar PCI-DSS, además se consultó el informe de cumplimiento de la industria de tarjetas de pago de 2014 publicado por Verizon, así como artículos académicos relacionados con el tema.

1. El estándar PCI en la industria de las tarjetas de pago.

El estándar PCI hace referencia al conjunto de requisitos operativos de carácter técnico definidos por la industria de las tarjetas de pago, con el fin de proteger los datos de los tarjetahabientes. Dicho estándar se aplica a todos los comerciantes y organizaciones que almacenan, procesan o transmiten estos datos, además de incluir normas específicas para los desarrolladores de software y fabricantes de aplicaciones, así como de dispositivos utilizados en las transacciones.
El estándar PCI fue desarrollado por las principales marcas de tarjetas de pago [2] quienes conformaron el consejo de estándares de seguridad PCI el cual está integrado por:

American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc.

En el mes de septiembre de 2006, se publicó la versión 1.1 del estándar PCI-DSS que tuvo vigencia hasta octubre de 2008 cuando fue publicada la versión 1.2, de la cual se generó la versión 1.2.1 en julio de 2009, en la que se realizaron algunas modificaciones al estándar; posteriormente en octubre de 2010 se publicó la versión 2.0, vigente hasta el mes de noviembre de 2013 donde fue publicada la versión 3.0, que es actualmente tomada como marco de referencia para adoptar los requisitos en la industria de las tarjetas de pago en el estándar PCI-DSS.

2. Componentes del estándar PCI

El estándar PCI [3] está orientado a las siguientes tres áreas:

PCI Data Security Standard*:* El estándar PCI-DSS es aplicable a cualquier entidad que almacena, procesa y transmite datos de los tarjetahabientes. Cubre los componentes técnicos y operativos del sistema incluidos la conexión a los datos de los tarjetahabientes. Si una empresa acepta o procesa datos de tarjetas de pago debe cumplir con el PCI-DSS.

PIN Transaction Security Requirements: El PTS PCI se aplica a los fabricantes quienes especifican y ponen en práctica las características de los dispositivos así como la gestión del número de identificación personal PIN en las terminales usadas para las transacciones financieras con tarjetas de pago.

Payment Application Data Security Standard: El estándar PA-DSS se aplica para los desarrolladores de software e integradores de aplicaciones que almacenan, procesan o transmiten datos de los titulares de las tarjetas. Rige a las aplicaciones que se venden, distribuyen o son licenciadas por terceros. No aplica para aplicaciones que son de uso exclusivamente interno y que no son comerciadas ya que estas están cobijadas por el estándar PCI-DSS

3. PCI-DSS

Con base a la información suministrada de PCI-DSS y sus componentes, a continuación se realiza un énfasis sobre los requisitos y mejores prácticas que se abordan en el mismo.

PCI-DSS es un estándar mundial de seguridad para proteger los datos de los tarjetahabientes, cualquier empresa que acepte tarjetas de pago debe cumplir sin importar su tamaño. Está conformado por 12 requisitos básicos [4], referidos a continuación y agrupados en 6 secciones conocidas como objetivos de control y se presentan como las mejores prácticas de seguridad en la industria de las tarjetas de pago:

a. Desarrollar y mantener redes y sistemas seguros: Se debe instalar y mantener la configuración de un *firewall* con el fin de proteger los datos, además de no utilizar parámetros de seguridad o contraseñas proporcionados por el proveedor con valores de fábrica.
b. Proteger los datos del titular de la tarjeta: El objetivo de este ítem es proteger los datos almacenados, así como cifrar la transmisión de los mismos a través de redes públicas.
c. Mantener un programa de administración de vulnerabilidad: Básicamente consiste en usar y actualizar regularmente un *software* antivirus, desarrollar y mantener sistemas y aplicaciones seguras.
d. Implementar medidas sólidas de control de acceso: Se busca restringir el acceso a los datos de los tarjetahabientes, tomando como base la necesidad del funcionario de conocer la información, así como evitar el acceso físico a los datos de los mismo; además se sugiere asignar un número de identificación único a cada persona con acceso a un computador en la organización.

e. Supervisar y evaluar las redes con regularidad: Se busca monitorear y rastrear todos los accesos a los recursos de red así como a los datos de los titulares de las tarjetas. Además se deben probar regularmente los sistemas y procesos de seguridad.
f. Mantener una política de seguridad de información: Consiste en mantener y divulgar a todo el personal una política que aborde la seguridad de la información.

4. Aplicabilidad del estándar PCI-DSS

El estándar PCI-DSS se aplica donde se almacenen, procesen o transmitan datos de cuentas. Se debe tener en cuenta que no solo aplica a entidades financieras, sino también en comercios, tales como supermercados y proveedores de servicios a manera de pasarelas de pago o fabricantes de tarjetas.

Los datos de las cuentas constan de los datos de los titulares de las tarjetas más los datos confidenciales de autenticación, como se muestra a continuación [5]:

Los datos de titulares de tarjetas incluyen:
- Número de cuenta principal PAN.
- Nombre del titular de la tarjeta.
- Fecha de vencimiento.
- Código de servicio.

Los datos confidenciales de autenticación incluyen:
- Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip).
- El dígito de verificación dependiendo de la marca de la tarjeta. CAV2/CVC2/CVV2/CID
- PIN/Bloqueos de PIN.

La siguiente tabla muestra el resumen de los datos de las tarjetas tanto del titular como confidenciales.

Tabla No.1 Datos de la Tarjeta.

	Dato	Almacenamiento permitido	Datos almacenados ilegibles
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	SI	SI
	Nombre del titular de la tarjeta	SI	NO
	Código de servicio	SI	NO
	Fecha de vencimiento	SI	NO
Datos confidenciales de autenticación	Contenido completo de la pista	NO	NO (Requisito 3.2)
	CAV2/CVC2/ CVV2/CID	NO	NO (Requisito 3.2)
	PIN/Bloqueo de PIN	NO	NO (Requisito 3.2)

Fuente: Normas de seguridad de datos de la PCI (industria de tarjetas de pago), versión 3.0 https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Se debe tener en cuenta que los requisitos del estándar PCI-DSS se aplican sólo si se almacena, procesa o transmite un número de cuenta principal (PAN), de lo contrario dichos requerimientos no aplican.
Cada marca de tarjetas ha definido niveles de validación del cumplimiento del estándar tanto en los comercios como en los proveedores de servicios según el nivel de transacciones y el riesgo del sistema de pago. Para determinar estos niveles, se

requiere realizar una auditoría en sitio anual por parte de un PCI QSA (*Qualified Security Assesor*).

Aquellas entidades que no estén obligadas a la auditoria, deberán elaborar un cuestionario de autoevaluación. Dicha evaluación se debe realizar sólo sobre los sistemas de la entidad que traten o transmitan este tipo de información.

5. Factores que afectan el cumplimiento del estándar PCI-DSS

Al implementar aplicaciones de pago seguro PA-DSS en un entorno que cumpla el estándar PCI-DSS, dichas aplicaciones pueden impedir su cumplimiento si se presenta alguna de las siguientes situaciones:

a. Almacenamiento de los datos de banda magnética o los datos equivalentes que se encuentran en el chip.
b. Inhabilitar características necesarias en el PCI-DSS, para que la aplicación de pago funcione correctamente, como por ejemplo inhabilitar el antivirus o el firewall.
c. El uso por parte de los proveedores de métodos inseguros para establecer conexión con la aplicación con el fin de proporcionar soporte al cliente.

Otros errores comunes que han sido identificados cuando se realizan evaluaciones de cumplimiento [6], incluyen entre otros:

a. Uso de datos de producción del titular de la tarjeta para fines de pruebas.
b. Fallo en el cifrado del número completo de la tarjeta de pago.
c. Ausencia de un sistema de segmentación de red que aísle el entorno de la transacción.
d. Falta de diferenciación de las obligaciones del personal interno.
e. Carencia de etiquetado de confidencial en los medios de difusión de datos del titular de la tarjeta.

La implementación del estándar PCI-DSS no debe convertirse en un problema para la organización, si bien es cierto que tiene componentes que pueden llegar a ser un reto, se debe entender que PCI-DSS debe ser parte de la actividad normal del negocio y sus procedimientos, y no entenderse como un requerimiento independiente [7].

6. El estado del cumplimiento del estándar PCI

Según un estudio realizado por *Forrester Consulting* [8], en nombre de la RSA y la división de seguridad EMC, con el fin de determinar las prioridades y retos en torno al estándar PCI en EEUU y Europa, se logró determinar que las organizaciones suelen almacenar mucha más información de las tarjetas de crédito que sólo los números de las mismas, además se estableció que las organizaciones que procesan un gran volumen de transacciones son las que más incurren en estas faltas.

En el estudio se consultaron 677 fuentes tanto en EEUU y Europa, sobre las prácticas de retención de información relacionadas con las tarjetas de crédito. El 94% de los encuestados era personal con

cargos directivos y el 68% de los encuestados de EEUU eran de organizaciones con ingresos superiores al billón de dólares.

A la pregunta ¿Qué tipo de datos de tarjetas de crédito almacena su compañía?, se obtuvieron los siguientes resultados:

Un 81% afirmó que almacenaba el número de la tarjeta de crédito, frente a un 73% que aseguró que guardaba en sus registros la fecha de expiración de las tarjetas. Del total de los encuestados un 71% aceptó que guardaba el código de verificación de las tarjetas y un 57% almacenaba la información de la banda magnética de la misma.

Otro estudio llevado a cabo por la empresa Verizon en el año 2014 [9], el cual tomó como referencia estudios anteriores y evaluaciones reales de PCI, enfocadas principalmente en 100 informes sobre cumplimiento, llevadas a cabo por asesores calificados de la compañía, mostró que los mayores niveles de ejecución de las compañías están enfocados a los siguientes requerimientos:

a. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas. (Requerimiento 4).
b. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. (Requerimiento 5).
c. Restringir el acceso físico a los datos del titular de la tarjeta. (Requerimiento 9).
d. Mantener una política que aborde la seguridad de la información de todo el personal. (Requerimiento 12).

Mientras que las compañías experimentaron mayores dificultades al cumplir con los siguientes requerimientos:

a. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores. (Requerimiento 2).
b. Proteja los datos del titular de la tarjeta que fueron almacenados. (Requerimiento 3).
c. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas. (Requerimiento 10).
d. Pruebe con regularidad los sistemas y procesos de seguridad. (Requerimiento 11).

La siguiente tabla muestra los resultados más relevantes con relación al cumplimiento de los requerimientos, que se obtuvieron con el estudio:

Tabla No.2 Resumen de Cumplimiento de los requerimientos del estándar PCI-DSS – Promedio

RESUMEN DE CUMPLIMIENTO PCI-DSS POR REQUERIMIENTO – PROMEDIO		
Requisito 1	Instale y mantenga una configuración de firewalls para proteger los datos de los titulares	86.4%
Requisito 2	No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los	81.4%
Requisito 3	Proteja los datos del titular de la tarjeta que fueron almacenados	79.3%
Requisito 4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas	87.8%
Requisito 5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus	95.9%
Requisito 6	Desarrolle y mantenga sistemas y aplicaciones seguras	87.4%
Requisito 7	Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la	86.8%
Requisito 8	Identificar y autenticar el acceso a los componentes del sistema	84.1%
Requisito 9	Restringir el acceso físico a los datos del titular de la tarjeta	94.9%
Requisito 10	Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las	82.2%
Requisito 11	Pruebe con regularidad los sistemas y procesos de	74.6%
Requisito 12	Mantener una política que aborde la seguridad de la información de todo el personal	89.7%

Fuente: Verizon 2014 PCI Compliance Report. http://www.verizonenterprise.com/pcireport/2014/

7. Conclusiones

Aun cuando algunos componentes del estándar PCI-DSS, suponen un reto para las organizaciones, la implementación de dicho estándar se debe ver como parte de la actividad normal y no como un requerimiento aislado.

Además, existe la errada creencia de que el modelo PCI-DSS es muy exigente, sin embargo la mayoría de requerimientos hacen referencia a buenas prácticas de seguridad que se pueden alinear con otros modelos de seguridad.

Por el hecho de que el estándar PCI-DSS es de obligatorio cumplimiento para las entidades que almacenan, procesan o transmiten información de cuentas de tarjetas, no se debe asumir que su implementación implique un trabajo duro y en algunos casos costoso; sino por el contrario verlo como una oportunidad para mejorar procesos internos que en definitiva beneficiarán a la organización en los temas relacionados con la seguridad de la información.

Muchas de las prácticas presentadas en el estándar PCI-DSS obedecen al sentido común, pero las ocupaciones cotidianas de la gestión corporativa en las empresas, en algunos casos ocasionan que los objetivos del estándar no se implementen de la forma adecuada, debido a que no existe un único método para lograrlo y se debe trabajar según las necesidades de cada organización.

Por lo tanto las empresas que decidan acogerse al estándar con el fin de mejorar su seguridad, deben identificar sus principales retos y prioridades en el momento de proteger los datos de sus tarjetahabientes.

Se espera que a través de este documento el lector tenga una visión más clara del estado actual del cumplimiento del estándar PCI-DSS en la industria de las tarjetas de pago y que le sirva como punto de referencia para lograr los objetivos propios de su organización.

Referencias

[1] Morsea, Edward A. Ravalb, Vasant. (2008). *PCI DSS: Payment card industry data security standards in context.* Disponible en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1303122&download=yes [Consultado febrero 14, 2015]

[2] Balcazar, Priscila. (2010). *Todo lo que necesita saber sobre PCI (Payment Card Industry Security Standards) y no se atrevía a preguntar.* Disponible en: http://www.magazcitum.com.mx/?p=590. [Consultado febrero 13, 2015]

[3] Security Standards Council. (2013). *PCI (industria de tarjetas de pago) Normas de seguridad de datos.* Disponible en: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf. [Consultado febrero 8, 2015]

[4] Security Standards Council. (2013). *PCI (industria de tarjetas de pago) Normas de seguridad de datos.* Disponible en: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf. [Consultado febrero 8, 2015]

[5] Security Standards Council. (2013). *PCI (industria de tarjetas de pago) Normas de seguridad de datos.* Disponible en: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf. [Consultado febrero 8, 2015]

[6] Rees, James. (2012). *Tackling the PCI DSS Challenges. Revista Computer Fraud & Security.* Disponible en: www.sciencedirect.com. [Consultado febrero 11, 2015]

[7] Forrester Consulting. (2007). *The State of PCICompliance, a study commissioned by RSA, the security division of EMC.* Disponible en: www.rsa.com/go/wpt/wpindex.asp?WPID=8778 [Consultado febrero 12, 2015]

[8] Forrester Consulting. (2007). *The State of PCICompliance, a study commissioned by RSA, the security division of EMC.* Disponible en: www.rsa.com/go/wpt/wpindex.asp?WPID=8778 [Consultado febrero 12, 2015]

[9] Verizon's team of Qualified Security Assessors (QSAs). (2014). *Verizon 2014 PCI Compliance Report*. Disponible en: http://www.verizonenterprise.com/pcireport/2014/. [Consultado febrero 10, 2015]

Christian Camilo Vanegas Pacheco. Ingeniero Electrónico graduado en el año 2007 de la Universidad Manuela Beltrán en la ciudad de Bogotá: Actualmente radicado en esta misma ciudad desempeñando el cargo de Ingeniero Preventa en Seguridad en la empresa Adistec de Colombia.