La norma PCI DSS[1]

Versión 3.21:

Definición de su objetivo y alcance.

[1] Realizado con el apoyo de IQ Information Quality www.iqcol.com

INTRODUCCION

PCI no es como tal una regulación. El término PCI se refiere al pago dentro de una industria determinada a través del uso de tarjetas crédito o débito (Payment Card Industry). Normalmente cuando nos referimos a las siglas PCI, queremos señalar el PCI Data Security Standard (DSS), actualmente en la versión 3.21. Pero, nos referiremos por brevedad en este artículo a la sigla PCI con el fin de identificar esta regulación de la industria la cual será verificadas a través de la realización de auditorías PCI de seguridad.

La norma PCI DSS (Payment Card Industry Data Security Standard) fue desarrollada por un conjunto de compañías de tarjetas de débito y crédito en el año 2006 entre las que estaban: America Express, Discover, JCB, Mastercard y VISA. De esta unión se creó el Payment Card Industry Security Standards Council (PCI-SSC), el cual es responsable de la creación, desarrollo, y difusión de la norma PCI DSS.

Las compañías autorizadas por el Concilio (PCI SSC) para realizar la validación de cumplimiento de la norma PCI DSS se conocen como QSA (Qualified Security Assessor), los cuales deben cumplir con una serie de requisitos como empresa y sus ingenieros deben ser entrenados directamente por esta asociación. La norma PCI es una de las normas más exigentes a nivel mundial en lo relacionado con la protección de la información sensible debido al énfasis que pone en los requerimientos de tipo tecnológicos y la rigurosidad que exige en el proceso de evaluación para otorgar la certificación de cumplimiento. La evaluación, para obtener la certificación, exige que el 100% de los requerimientos y sub-requerimientos (aproximadamente son 350) estén implementados correctamente.

PCI DSS procura que las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes protejan esta información con el fin de evitar fugas que involucren divulgación de información sensible. Este tipo de fugas podría afectar todo el ecosistema de tarjetas de pago incluyendo clientes, comercios e instituciones financieras. Estas entidades perderían credibilidad como consecuencias de fugas de información y quedarían expuestas a numerosas demandas económicas y en algunos casos su supervivencia en el tiempo quedaría seriamente comprometida.

Lograr el cumplimiento de PCI DSS es fundamental para el éxito a largo plazo de las organizaciones que procesan información sensible o realizan pagos con tarjetas. El cumplimiento involucra la identificación continua de amenazas y vulnerabilidades que podrían potencialmente afectar a dichas organizaciones. La mayoría de ellas nunca se recuperan

totalmente de una infracción o fuga de sus datos ya que la pérdida o el impacto es mayor que los datos en sí mismos. Seguir la norma PCI es una gran oportunidad para realizar más negocios de manera segura. Por medio de esta norma se logra asegurar la salud y confianza en las transacciones de pago para cientos de millones de personas en el mundo que utilizan medios electrónicos para sus transacciones.

ESTRUCTURA DE LA NORMA PCI

Todas las industrias normalmente evolucionan, la industria de medios de pagos no es la excepción. La tecnología, por su parte, mantiene también un ritmo acelerado de cambios como, por ejemplo: nuevas funcionalidades en los sistemas operativos, nuevas tecnologías de seguridad en los firewalls y dispositivos de protección de red, aplicaciones con funcionalidades que mejoran la experiencia del usuario, información almacenada en la nube, nuevas tecnologías de acceso a los sistemas (celulares, tabletas, etc.), entre otras.

Esta evolución inherente a la tecnología ofrece nuevas oportunidades de facilidad de acceso a la información, a la vez que expone a las organizaciones a nuevos riesgos de fugas de información. Es aquí donde la norma PCI ofrece la rigurosidad requerida para controlar los nuevos retos a los que las nuevas tecnologías nos exponen. Para lograr el objetivo de proteger la información sensible, PCI propone doce requerimientos que cubren los aspectos más significativos en donde la seguridad debe ser considerada. A continuación, en la siguiente tabla, se presentan estos requerimientos:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Figura 1. Requerimientos de la norma.

PROCESO DE CUMPLIMIENTO

Dependiendo del tipo de compañía se requerirá de pasar por una auditoría PCI cada año o completar un cuestionario de auto-evaluación con el fin de poder validar el cumplimiento de dicha auditoría. Además de esta actividad, se tendrán que presentar los resultados trimestrales del análisis de vulnerabilidades del perímetro de red (el cual tiene que ser realizado por un fabricante debidamente certificado para la realización de auditorías PCI), el cual es evidencia del desarrollo y completitud de esta actividad. Se busca con estas pruebas de vulnerabilidad demostrar que su compañía posee las mejores prácticas en lo relacionado con la remedición y la gestión de vulnerabilidades. Este será, pues, el objetivo principal de la auditoría PCI.

EVOLUCIÓN DE PCI DSS

PCI DSS es el estándar el cual se ha desarrollado a través de los esfuerzos varias asociaciones de tarjetas. En 1990, estas asociaciones de tarjetas desarrollaron varios estándares con el fin de mejorar la seguridad de la información confidencial que es transmitida o procesada por estas entidades. En el caso de VISA, diferentes regiones vinieron con diferentes estándares. Luego, en Junio del 2001, VISA Estados Unidos, lanzó el Cardholder Information Security Program (CISP). El CISP, como proceso de auditoría PCI en la versión 1.0 fue inspiración por el desarrollo del PCI DSS. El proceso de auditoría PCI fue recorriendo diferentes versiones hasta llegar a la 2.3 en Marzo del 2004. En este momento, VISA estaba trabajando en conjunto con Master Card. Esto conllevó a la propuesta de que los diferentes establecimientos debían recorrer el camino del cumplimiento de acuerdo a lo establecido por el CISP, es decir, seguir los lineamientos de la auditoría de seguridad, junto con las directrices de MasterCard para el análisis de vulnerabilidades. Visa mantendría así la lista de los asesores aprobados y MasterCard mantendría la lista de los fabricantes aprobados de dispositivos de analisis de redes (scanning vendors). Finalmente el PCI se conformaría: https://www.pcisecuritystandards.org. Compuesto por American Express, Discover Financial Services, JCB, MasterCard, VISA, PCI Co, mantendría la propiedad intelectual del DSS.

ASESORES APROVADOS Y FABRICANTES CERTIFICADOS

PCI, ahora controla qué compañías le son permitidas conducir una auditoría PCI. Estas compañías, conocidas oficialmente como *Qualified Security Assesor* (QSA), deben recorrer un proceso de aplicaciones y calificaciones con el fin de demostrar su cumplimiento a través de la calidad de sus procesos operativos y administrativos. Los QSA también deben invertir

en entrenamiento y certificación del personal con el fin de construir un equipo de *Qualified Security Assesors* (QSAs), capacitado para realizar las auditorías PCI.

Por otro lado, para llevar a ser un Approved Scanning Vendor (ASV), estas compañías deben recorrer un proceso similar al de los QSAC. La diferencia radica que en el caso de los QSA, los cuales deben atender entrenamientos periódicos y anuales, los ASVs deben enviar (submit) un informe de resultados contra un perímetro de red. Una compañía puede elegir ser tanto QSA como ASV, lo que le permitirá ser un único fabricante en capacidad de ofrecer la auditoría completa PCI.

ANEXOS

Card Brand	Additional Program Information
American Express	Web: www.americanexpress.com/datasecurity E-mail: American.Express.Data.Security@aexp.com
Discover	Web: www.discovernetwork.com/resources/data/data_security.html E-mail: askdatasecurity@discoverfinancial.com
JCB	Web: www.jcb-global.com/english/pci/index.html E-mail: riskmanagement@jcbati.com
MasterCard	Web: www.mastercard.com/sdp E-mail: sdp@mastercard.com
Visa USA	Web: www.visa.com/cisp E-mail: cisp@visa.com
Visa Canada	Web: www.visa.ca/ais

Figura 2. Entidades que conforman el concilio.

PCI Security Standards Council

PCI DSS Applicability Information

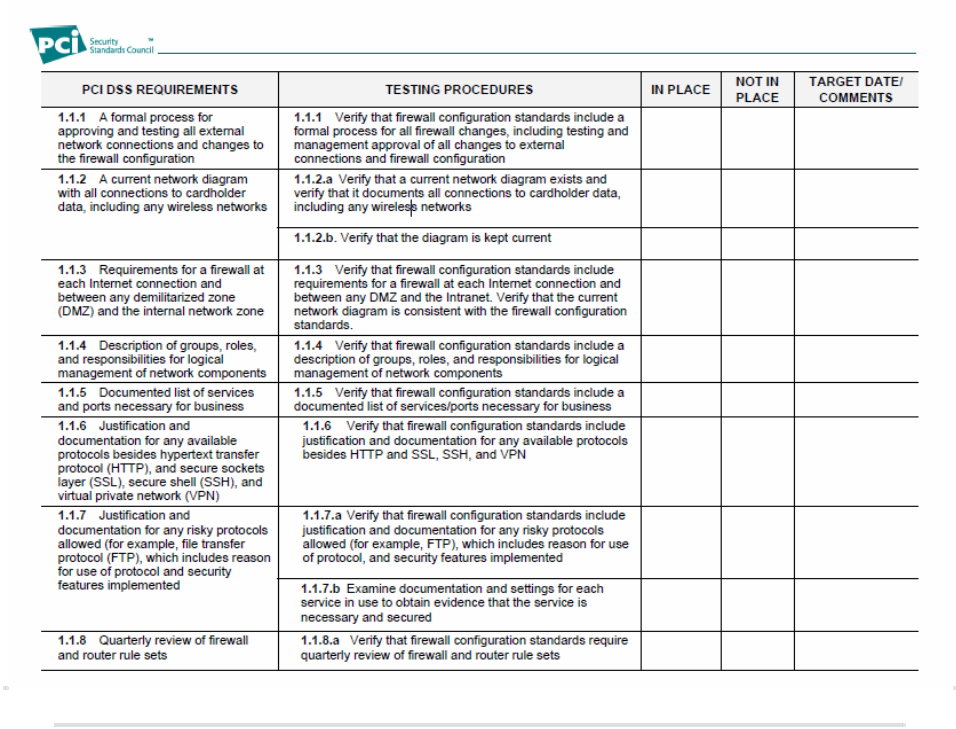
The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether **storage** of each data element is permitted or prohibited; **and if each data element** must be **protected**. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

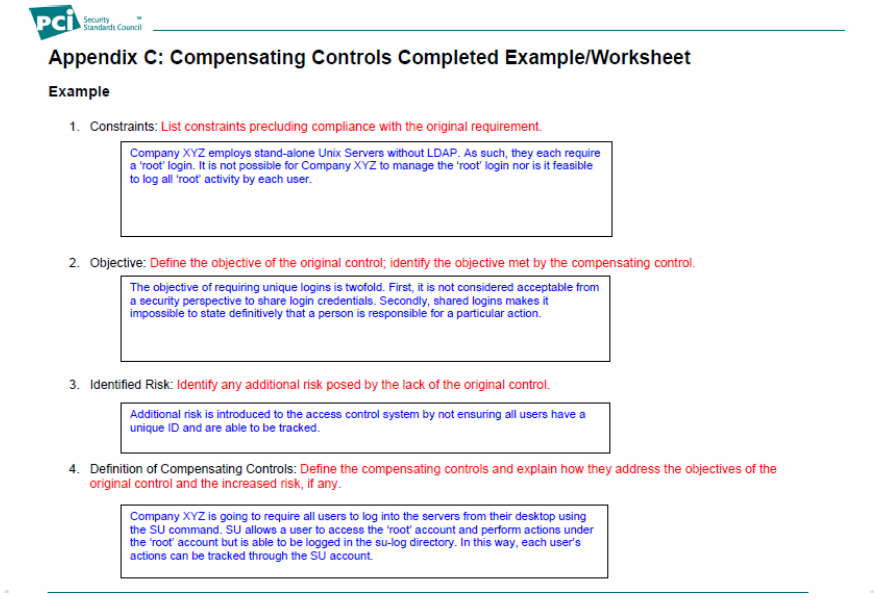
** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Figura 3. Información de aplicabilidad de la auditoría PCI.



PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	**1.1.1** Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			
	1.1.2.b. Verify that the diagram is kept current			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the Intranet. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components			
1.1.5 Documented list of services and ports necessary for business	**1.1.5** Verify that firewall configuration standards include a documented list of services/ports necessary for business			
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	**1.1.6** Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN			
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	**1.1.7.a** Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol, and security features implemented			
	1.1.7.b Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured			
1.1.8 Quarterly review of firewall and router rule sets	**1.1.8.a** Verify that firewall configuration standards require quarterly review of firewall and router rule sets			

Figura 4. Ejemplo de lista de verificación de la red para realizar la auditoría PCI.



Appendix C: Compensating Controls Completed Example/Worksheet

Example

1. Constraints: List constraints precluding compliance with the original requirement.

   Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a 'root' login. It is not possible for Company XYZ to manage the 'root' login nor is it feasible to log all 'root' activity by each user.

2. Objective: Define the objective of the original control; identify the objective met by the compensating control.

   The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, shared logins makes it impossible to state definitively that a person is responsible for a particular action.

3. Identified Risk: Identify any additional risk posed by the lack of the original control.

   Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.

4. Definition of Compensating Controls: Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.

   Company XYZ is going to require all users to log into the servers from their desktop using the SU command. SU allows a user to access the 'root' account and perform actions under the 'root' account but is able to be logged in the su-log directory. In this way, each user's actions can be tracked through the SU account.

Figura 5. Controles compensatorios de la auditoría PCI.