Artículo de investigación

Implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago en una procesadora de tarjetas

Implementation of the Payment Card Industry Data Security Standard in a card processor

Revista sobre estudios e investigaciones del saber

Fanny Carolina Mujica Fernández [1]
https://orcid.org/0000-0003-3452-039X
[1] Universidad Nacional del Asunción. Facultad Politécnica. Asunción, Paraguay. mujicafanny@fpuna.edu.py

Mario Roberto Monges Olmedo † [2]
https://orcid.org/0000-0002-7413-1789
[2] Universidad Nacional del Asunción. Facultad Politécnica. Asunción, Paraguay. mario.monges@pol.una.py

Resumen

Como resultado del aumento del fraude y el robo de identidad de las tarjetas de pago, las cinco marcas principales de tarjetas de pago se unieron para formar el Consejo de Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard o sus siglas en inglés PCI SSC). Este Consejo desarrolló los requisitos del Estándar de Seguridad de Datos en la Industria de Pagos, a fin de fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad; dicho estándar aplica a todas las entidades que almacenan, procesan o transmiten datos confidenciales y/o de autenticación del tarjetahabiente. El enfoque de la investigación es cualitativo. El nivel de investigación planteado es el exploratorio y descriptivo, en cuanto al diseño la misma fue no experimental y de corte transversal. La unidad de análisis incluyo a doce (12) colaboradores de la Procesadora de tarjetas. En este trabajo se implementa el estándar PCI DSS en una procesadora de tarjetas, con el fin de fortalecer los esquemas de seguridad y protección de la información del tarjetahabiente. Como resultado de esta implementación se eleva el nivel de seguridad, se reduce el riesgo de pérdida de información y se garantiza el cumplimiento de la operabilidad con las diferentes marcas de medios de pago.

Palabras Claves: Industria de Tarjeta de Pago. Estándar de Seguridad de Datos. Consejo de Normas de Seguridad PCI. Tarjetahabiente. Tarjetas de pago.

Abstract

As a result of the rise in payment card fraud and identity theft, the five major payment card brands have come together to form the PCI Security Standards Council (PCI SSC). This Council developed the requirements of the Data Security Standard in the Payment Industry, in order to promote and improve the security of cardholder data and facilitate the adoption of security measures; This standard applies to all entities that store, process or transmit confidential and/or cardholder authentication data. The research approach is qualitative. The level of research proposed is exploratory and descriptive, in terms of design it will be non-experimental and cross-sectional. The analysis unit included twelve (12) employees of the Card Processor. In this work, the PCI DSS standard is implemented in a card processor, in order to strengthen the security schemes and protection of the cardholder's information. As a result of this implementation, the level of security is raised, the risk of information loss is reduced and compliance with the operability with the different means of payment brands is guaranteed.

Keywords: Payment Card Industry. Data Security Standard. PCI Security Standards Council. Cardholder. Payment cards.

Área del conocimiento: Ingeniería y Arquitectura
Correo de Correspondencia: mujicafanny@fpuna.edu.py
Conflictos de Interés: Los autores declaran no tener conflictos de intereses.

Fecha de recepción: 26/04/2022 Fecha de Aprobación: 18/10/2022
Página Web: http://publicaciones.uni.edu.py/index.php/rseisa

Citación recomendada: Mujica Fernández, F. C.; Monges Olmedo, M. R. (2023). Implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago en una procesadora de tarjetas. Revista sobre estudios e investigaciones del saber académico (Encarnación), 17(17): e2023005

Introducción

Con el aumento de los servicios y operaciones digitales se propulsó y facilitó el acceso a tarjetas de crédito/débito y prepagas. Las mismas representan múltiples ventajas a la hora de realizar distintas transacciones en cajeros, Puntos de Ventas (Point Of Sales o su sigla en inglés POS), entidades financieras, portales de internet y aplicaciones móviles; sin embargo, los riesgos asociados a las nuevas tecnologías para los tarjetahabientes como el robo de identidad y los fraudes en varias modalidades representan un enorme desafío para los procesadores de tarjetas, bancos, entidades financieras y para los comerciantes en general.

Dada la escasa conciencia acerca de la seguridad en medios de pago y los altos índices de fraude en tarjetas de crédito y débito, la procesadora de tarjetas es consciente de que debe brindar a los comercios adheridos y a los usuarios de la plataforma, la seguridad de que la tecnología que utilizan para realizar sus operaciones se encuentra acorde a los requisitos internacionales, que éstas sean robustas y seguras, por lo cual deben mejorar sus procesos y procedimientos para prevenir potenciales fraudes o robos, así como también mitigar los riesgos en las transacciones con tarjetas de pago y proteger datos sensibles, teniendo como base el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard o sus siglas en inglés PCI DSS).

La procesadora de tarjetas es una empresa de Servicios, vinculada a personas, empresas, entidades financieras, organizaciones e instituciones privadas y públicas en el negocio de transacciones electrónicas, consistentes en la comercialización de servicios de red electrónica de transferencias a varios tipos de entidades y comercios, a través del procesamiento de tarjetas de crédito/débito, instalación de equipos, red de POS, de cajeros automáticos, y también en e-commerce, entre otros. Su oficina se encuentra ubicada en la ciudad de Asunción. Desde sus inicios ha participado de proyectos de gran envergadura a nivel de seguridad transaccional.

El Consejo de Estándar de Seguridad PCI

Las organizaciones no solo necesitan proteger la información del consumidor que está siendo procesado, transmitido o almacenado por los emisores, adquirentes, comerciantes y/o proveedores de servicios, sino que también deben considerar la protección de la reputación de la marca.

Es por esto que principios del año 2000, Visa creaba el Programa de Seguridad de la Información de la Cuenta para Visa Internacional (Visa Inc., 2000) y el Programa de Seguridad de la Información del Titular de la Tarjeta para USA (Visa USA, 2001). De igual manera MasterCard impuso el Programa de Protección de datos (Mastercard, 2001), junto con la Política Operativa de Seguridad de Datos de American Express (American Express, 2000), en tanto Discover tenía el Programa de Cumplimiento y Seguridad de la Información Discover (Discover Global Network, 2000) y JCB Internacional tenía el Programa de Seguridad de Datos (JCB Co., 2000). De modo que cada marca tenía programas de seguridad individuales, pero estos esfuerzos eran descoordinados y dificultaba su implementación para una organización que procesara diferentes tipos de tarjetas.

En el año 2006, luego de las enormes pérdidas económicas producidas como consecuencia del aumento en el fraude de tarjetas de crédito, y el robo de identidad, las cinco marcas principales de tarjetas (VISA, MasterCard, Discover, American Express, JCB) que ya contaban con sus propios requisitos de seguridad de datos, se unieron para unificar los estándares y formar el PCI Security Standards Council (PCI SSC) (PCI SSC, 2006), donde se centralizaron las mejores características de cada programa de seguridad de dichas marcas, facilitando su adopción, control y mejora continua.

PCI SCC es un foro mundial, cuyo principal objetivo de definir los controles de seguridad orientados hacia la protección de los datos de tarjetas de pago durante todo el flujo transaccional (PCI Security Standards Council LLC, 2006). Cuyas principales incumbencias son: Aprobación de cumplimiento, Seguimiento y exigencia del cumplimiento, Definiciones de quienes deben cumplir.

El PCI SSC proporciona programas de capacitación especificas a asesores, homologación de empresas para auditorias y servicios y documentación complementaria, además de desarrollar y mantener estándares tales como: Estándar de Seguridad de Datos de PCI (Payment Card Industry Data Security Standard o su siglas en inglés PCI DSS), Estándar de Seguridad de Datos de Aplicación de Pago

(Payment Card Industry Payment Application Data Security Standard o su sigla en inglés PA-DSS), Estándar de Seguridad de Transacción de PIN (PIN Transaction Security o su sigla en inglés PTS), Estándar de Proveedores de servicios de token (Payment Card Industry Token Service Providers o su siglas en inglés PCI TSP), Estándar de entrada de PIN basado en software en un dispositivo comercial disponible (Payment Card Industry Software based PIN Entry on COTS o su siglas en inglés PCI SPoC), Estándar Punto a Punto Cifrado (Payment Card Industry Point-to-Point Encryption o su siglas en ingles P2PE) y el recientemente desarrollado, el Estándar de seguridad del Software (Payment Card Industry 3-D Secure o su siglas en siglas PCI 3DS) (PCI Security Standards Council, PCI Security Standards Council, 2006).

El Estándar de Seguridad PCI DSS

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) se desarrolló para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas.

La PCI DSS comprende un conjunto mínimo de requisitos para proteger los datos de cuentas y se puede mejorar por medio de controles y prácticas adicionales a fin de mitigar los riesgos, así como leyes y regulaciones locales, regionales y sectoriales. Además, los requisitos de la legislación o las regulaciones pueden requerir la protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de tarjeta). El estándar PCI-DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales (PCI Security Standards Council LLC., 2018).

La versión del estándar PCI-DSS 3.2.1, fue lanzado en mayo de 2018 y entró en vigencia el 1 de enero de 2019, esta versión remueve las referencias de fechas que incluían una serie de requisitos identificados temporalmente como “buenas prácticas” y se estipularon como “requisitos obligatorios”

Se actualiza el ANEXO A.2: “Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana” donde se menciona que todas las entidades deben usar de forma obligatoria TLS v.1.2 o superiores en sus conexiones (PCI, 2018).

La PCI DSS consta de seis objetivos principales, que son conocidos como “objetivos de control” divididos en 12 requisitos específicos. Que se pueden observar en la Tabla 1 (PCI Security Standards Council LLC., 2018).

Tabla 1

Estándar de Seguridad de Datos de la de la Industria de Tarjetas de Pago, 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

Cada objetivo de control tiene requisitos secundarios y algunos tienen requisitos en varios niveles.

Los requisitos no son lineales ni secuenciales; Varían en naturaleza, alcance y granularidad. Algunos requisitos (por ejemplo, el requisito 1 - mantener firewall y requisito - 4, cifrar la transmisión) son preceptivos, mientras que otros (por ejemplo, el requisito 3 - proteger los datos almacenados y el requisito 6 - desarrollar y mantener sistemas seguros) son normativos en el sentido de que dejan los medios particulares de implementación de protección y seguridad a la entidad responsable del cumplimiento (Morsea & Ravalb, 2008).

La aplicabilidad de la Norma PCI DSS

¿Cuándo son aplicables los requisitos del estándar PCI DSS?

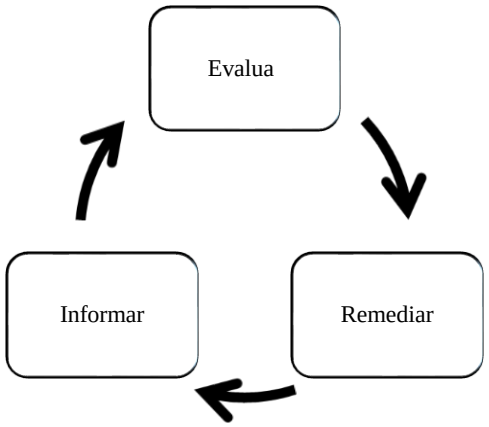
El estándar PCI DSS se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago (tanto antes como después de la autorización), entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, que arriesgan la perdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de franquicias), enfrentar auditorias rigurosas o pagos de multas y deben validar su cumplimiento al estándar en forma periódica.

Para lograr el cumplimiento del estándar PCI DSS, una organización debe cumplir todos los requisitos de la PCI DSS, independientemente del orden en que se cumplen.

El cumplimiento del estándar PCI DSS es un proceso continuo como se puede observar en la Figura 1 (Council, 2016).

Figura 1

Proceso de cumplimiento del Estándar PCI DSS



Las validaciones son realizadas por los Evaluadores de seguridad certificados (Quality System Assessment o su sigla en inglés QSA) y los Proveedores aprobados de escaneo (Approved Scanning Vendor o su sigla en inglés ASV) certificados por el PCI Security Standards Council.

Un error común en el ámbito del entorno de datos del titular de la tarjeta es incluir solo las áreas que almacenan, procesan o transmiten datos después de la autorización.

El número de cuenta principal es el factor que define los datos del titular de la tarjeta. Si estos datos se almacenan, procesan o transmiten con el número de cuenta principal (Primary Account Number o su sigla en inglés PAN) o se encuentran presentes de algún otro modo en el entorno de datos del titular de la tarjeta, se deben proteger de conformidad con los requisitos aplicables del Estándar PCI DSS

Los datos del titular de la tarjeta y los datos de autenticación confidenciales se definen según lo establecido en el Estándar PCI DSS (PCI Security Standards Council LLC., 2018).

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)
- CAV2/CVC2/CVV2/CID
- PIN/Bloqueos de PIN

Los datos de titulares de tarjetas y los datos de autenticación confidenciales que habitualmente se utilizan; independientemente de que esté permitido o no almacenar dichos datos y de que esos datos deban estar protegidos se pueden observar en la Tabla 2 (PCI Security Standards Council LLC., 2018).

Tabla 2.

Ilustra los elementos de los datos de titulares de tarjetas y los datos de autenticación confidenciales

		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 [1]	Contenido completo de la pista [2]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID [3]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN [4]	No	No se pueden almacenar según el Requisito 3.2

1. No se deben almacenar los datos de autenticación confidenciales después de la autorización (incluso si están cifrados).
2. Contenido completo de la pista que se encuentra en la banda magnética, datos equivalentes que se encuentran en el chip o en cualquier otro dispositivo
3. La cifra de tres o cuatro dígitos en el anverso o reverso de la tarjeta de pago
4. El número de identificación personal ingresado por el titular de la tarjeta durante una transacción con tarjeta presente o el bloqueo de PIN cifrado

Los requisitos 3.3 y 3.4 del Estándar PCI DSS sólo se aplican al PAN. Si el PAN se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN debe ser ilegible de acuerdo con el requisito 3.4 del Estándar PCI DSS. No se deben almacenar los datos confidenciales de autenticación después de la autorización, incluso si están cifrados. Esto se implementa aun cuando no haya PAN en el entorno (PCI Security Standards Council LLC., 2018).

Materiales y Métodos

El enfoque de la investigación es cualitativo. El nivel de investigación planteado es el exploratorio (se trabajará con fuentes secundarios) y descriptiva, pues se buscará detallar característica del fenómeno estudiado.

Según Roberto Hernández Sampieri: El enfoque cualitativo utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación (Hernández, Fernández , & Baptista, 2010).

Los estudios descriptivos buscan especificar las propiedades y las características importantes de cualquier fenómeno que se analice Describe tendencias de un grupo o población (Hernández, Fernández , & Baptista, 2010).

En cuanto al diseño la misma será no experimental puesto que no se manipularán la variable para obtener los datos de la investigación y de corte transversal ya que los datos serán recolectados en un solo momento de una sola vez.

La investigación no experimental se realiza sin la manipulación deliberada de las variables y en los que sólo se observan los fenómenos en su ambiente natural para analizarlos (Hernández, Fernández , & Baptista, 2010).

Durante la inspección realizada en la Procesadora de Tarjetas en la Ciudad de Asunción – Paraguay, se procedió a la entrevista del Gerente de TIC, Encargado de Infraestructura, Encargado de Producción, Encargado de Seguridad de la

Información, Encargado de Desarrollo, Encargado de RRHH, Encargado de Entidades y del Encargado de Operaciones, ya que en su trabajo está la operación, el manejo y el desarrollo de todos los procesos que están dentro del alcance de la norma de seguridad de datos en la industria de tarjetas de pago. El ámbito de esta revisión tuvo como alcance los siguientes ítems: operaciones de captura de transacciones vía ATM y POS de las marcas internaciones, Visa, Visa Electron, Mastercard y Maestro y todos los procesos asociados a éstas.
Se ha realizado un análisis de toda documentación y evidencia de los procedimientos aplicados por la procesadora de tarjeta, en cada uno de los requerimientos del Estándar PCI DSS V3.2.1 y los objetivos de control, las cuales comprenden:

- Redes y sistemas seguros
- Protección de datos del titular
- Administración de Vulnerabilidades
- Control de acceso
- Políticas de seguridad

Luego del análisis de la documentación de estos procesos, se comprueba el cumplimiento o no, de los mismos en relación a lo requerido por el Estándar PCI DSS.

Resultados

Luego de llevar a cabo la revisión de todas las documentaciones existentes, fue posible determinar que la Procesadora de Tarjetas se encuentra en cumplimiento al Estándar PCI DSS según se puede observar en la Tabla 3.

Tabla 3
Reporte de Cumplimiento

Requerimientos PCI DSS	Resumen de resultados (marque uno)		
	Cumple	No Cumple	No Aplica
1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.	X		
2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.	X		
3. Proteja los datos del titular de la tarjeta que fueron almacenados	X		
4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	X		
5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente	X		
6. Desarrollar y mantener sistemas y aplicaciones seguros	X		
7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	X		
8. Identificar y autenticar el acceso a los componentes del sistema.	X		
9. Restringir el acceso físico a los datos del titular de la tarjeta.	X		
10. Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta	X		
11. Probar periódicamente los sistemas y procesos de seguridad.	X		

12.	Mantener una política que aborde la seguridad de la información para todo el personal	X

Por otro lado, a fin de fortalecer, aumentar y mejorar la calidad y seguridad de los procesos, se recomienda lo siguiente:

- Plan de Contingencia: determinar la cantidad mínima de puestos de trabajos necesarios y recursos requeridos para el correcto funcionamiento del negocio en caso de una contingencia real.
- Análisis de Riesgos:
  - ✓ Identificar los riesgos asociados con delitos informáticos, ataques web, malware, Ransomware etc.
  - ✓ Realizar evaluaciones anuales que permitan a la Procesadora de Tarjeta estar actualizada en lo que respecta a cambios organizativos y a las cambiantes amenazas, tendencias y tecnologías.
- Determinar responsabilidades:
  - ✓ Dar a conocer a todo el personal los lineamientos de seguridad asociados, de manera a evitar que las defensas y los controles implementados sean ineficaces a causa de errores y/o acciones intencionales.
  - ✓ Implementar un procedimiento para que todo el personal sepa que no debe almacenar ni copiar datos del titular de la tarjeta en sus computadoras personales locales ni otros medios.

Discusión

Antes de la implementación del Estándar PCI DSS V3.2.1 dentro de la Procesadora de tarjetas, se hallaron Políticas, Normas y Procedimientos que no se encontraban formalizados y/o debidamente documentados; así como no conocían donde se encontraban todos los datos del titular de la tarjeta, lo cual dificultaba definir el alcance de los procesos para tener en cuenta.

La implementación permitió un cambio en los hábitos de todo el personal, proporcionó la ubicación de todos los datos del tarjetahabiente y de esta forma tomar conciencia acerca de proteger esos datos y fortalecer los mecanismos de seguridad de dicha información, la implementación mejoró la imagen corporativa lo cual se traduce como una estrategia de negocio ante posibles nuevos inversores y/o clientes. Pero sobre todo a obtener el compromiso y el apoyo de la alta gerencia, el directorio y todas las áreas involucradas en el proceso de certificación, ya que la certificación PCI DSS no es una certificación de seguridad, sino del negocio, por tanto, afecta a toda la Procesadora

Conclusión

Adherirse a los requisitos de la PCI DSS puede parecer una tarea muy confusa y compleja. Sin embargo, el cumplimiento del estándar proporcionó muchos beneficios a la procesadora de tarjeta, como ser: un adecuado nivel de seguridad que garantice la protección de los datos de tarjeta, mejorar la imagen de la marca mejorando la confianza de sus clientes en cuanto al tratamiento de sus datos sensibles, la aplicabilidad de nuevas estrategias de negocio dado que los clientes tienen las garantías de seguridad a la hora de tratar sus datos.

Todos los empleados de la procesadora de tarjeta colaboran mutuamente a fin de formar parte de una Política de Seguridad de la Información de manera a prevenir violaciones de seguridad y el robo de datos sensibles.

La implementación del Estándar mejoró el rendimiento de los procesos, por lo que exige la innovación en los procesos de seguridad, tecnologías y tratamiento de la información.

Referencias Bibliográficas

American Express. (2000). *American Express*. Obtenido de https://merchant-channel.americanexpress.com/merchant/en_US/data-security

Council, P. S. (2016). *El Enfoque Prioritario para Lograr el Cumplimiento de la PCI DSS.*

Discover Global Network. (2000). Obtenido de https://www.discoverglobalnetwork.com/solutions/pci-compliance/discover-information-security-

compliance/#:~:text=The%20Discover%20Information%20Security%20%26%20Compliance,the%20Discover%C2%AE%20Global%20Network.

Hernández, R., Fernández , C., & Baptista, L. (2010). *Metodología de la Investigación.* México: Mc GrawHill Educación.

JCB Co. (2000). *Global JCB*. Obtenido de https://www.global.jcb/en/products/security/data-security-program/index.html

Mastercard. (2001). *Mastercard*. Obtenido de https://www.mastercard.com/global/en/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI.html

Morsea, E. A., & Ravalb, V. (2008). PCI DSS: Payment card industry data security standards in context. *Elsevier*, 550.

PCI Security Standards Council LLC. (2018). *PCI DSS Requisitos y procedimientos de evaluación de seguridad.* PCI Security Standards Council LLC.

PCI Security Standards Council. (2006). *PCI Security Standards Council*. Obtenido de https://www.pcisecuritystandards.org/document_library

PCI Security Standards Council. (2006). *PCI Security Standards Council*. Obtenido de https://www.pcisecuritystandards.org/about_us/

PCI Security Standards Council LLC. (2006). *PCI Security Standards Council*. Obtenido de https://es.pcisecuritystandards.org/minisite/env2/

PCI SSC. (2006). *PCI Security Standards Council*. Obtenido de https://www.pcisecuritystandards.org/about_us/

Visa Inc. (2000). *Visa Inc.* Obtenido de https://www.visa.gp/run-your-business/small-business-tools/information-security/ais-program.html

Visa USA. (2001). *Visa Usa*. Obtenido de https://usa.visa.com/support/small-business/security-compliance.html