UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

“ANÁLISIS DE LA IMPLEMENTACIÓN DEL ESTÁNDAR PCI-DSS EN LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE UNA INSTITUCIÓN FINANCIERA”

AUTOR/A (S):

ZOILA ALEXANDRA CALLE PARRALES

ANDREA JACQUELINE MEJÍA VILLEGAS

DIRECTOR:

MG. EDUARDO NAVARRETE FERNÁNDEZ

GUAYAQUIL, ABRIL DEL 2015

DECLARATORIA DE RESPONSABILIDAD

Nosotras, Zoila Alexandra Calle Parrales y Andrea Jacqueline Mejía Villegas autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Guayaquil, Abril del 2015.

_____	_____
Zoila Alexandra Calle Parrales.	Andrea Jacqueline Mejía Villegas.
CC. 0929814267	CC. 0922638572

DEDICATORIA

Dedico este trabajo a Dios, que es el motor de mi vida, por bendecirme y darme la fortaleza necesaria para cumplir mis metas. A mis abuelos, mis padres y mis hermanos, por brindarme su amor y apoyo incondicional, porque han sido ejemplo de lucha y perseverancia, por alentarme y estar a mi lado siempre, porque han hecho de mí la mujer que soy, a ustedes mí más sincero agradecimiento.

A mis profesores durante esta carrera por compartir conmigo sus conocimientos y prepararme para enfrentar los retos profesionales que se me presenten en el ámbito laboral, por ir más allá del aspecto académico y otorgarme su sincera amistad a cada uno de ellos les dedico mi tesis.

Zoila Alexandra Calle Parrales

DEDICATORIA

Dedico principalmente este trabajo a Dios por ser mi guía, y enviarme a las personas más grandes de mi vida que son mis padres, mis hermanos y mis sobrinos por su apoyo incondicional e hicieron todo lo posible para que yo pudiera lograr mis sueños, por motivarme y darme la mano en esos momentos difíciles, a ustedes mi corazón y agradecimiento eterno.

A todos los docentes de mi carrera por su enseñanza académica que en este andar por la vida influyeron con su experiencia, en formarme como una persona preparada para los retos que se presentan en la vida a cada uno de ellos les dedico cada una de estas páginas de mi tesis.

Andrea Jaqueline Mejía Villegas.

AGRADECIMIENTO

A la Universidad Politécnica Salesiana por su apoyo y colaboración institucional para la realización de esta Tesis.

Durante estos años, son muchas las personas que han participado en nuestra formación académica. Agradecemos a los docentes los cuales siempre han demostrado su entrega a la vocación Salesiana, a los miembros del consejo de carrera, que nos apoyaron en este proceso.

Este proyecto es el resultado del esfuerzo en conjunto de todos los que formamos parte de este trabajo. Por esto agradecemos al director de Tesis Mg. Eduardo Navarrete Fernández.

Agradecemos a quienes que de una u otra forma estuvieron apoyándonos durante este proceso, porque cada uno aportó con sus enseñanzas; y es por ello que a cada uno de ustedes les dedicamos todo el esfuerzo y sacrificio que entregamos en la tesis.

Zoila Alexandra Calle Parrales.

Andrea Jacqueline Mejía Villegas.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo propone el análisis de la implementación del estándar de seguridad de datos para la industria de tarjetas de pago, conocido por su siglas en inglés PCI-DSS (Payment Card Industry – Data Security Standard), como medida de seguridad para prevenir fraudes en las transacciones que impliquen el uso de tarjetas de crédito y débito, como ayuda al cumplimiento de las exigencias de la Superintendencia de Bancos y Seguros respecto al procesamiento de las mismas.

Este estándar exige máxima seguridad en los datos de titular o dueño de la tarjeta, por lo tanto la idea de implementar PCI-DSS se enfoca en proteger y salvaguardar información sensible y confidencial, permitiéndole a la institución financiera (ya sea esta un banco, Cooperativa y otros proveedores de servicios) garantizar la seguridad de los datos de sus clientes. El enfoque del presente documento hace referencia al análisis de la implementación del Estándar PCI-DSS en un banco localizado en la ciudad de Guayaquil.

El análisis de la implementación del estándar PCI- DSS, abarca desde la definición conceptual, funcionalidad, requerimientos y actores que lo componen hasta la determinación de mejores prácticas de Seguridad que debe aplicar el banco para la implementación de mismo.

En el desarrollo de este proyecto de análisis se toma como estudio los mecanismos de seguridad que posee determinado banco ubicado en la ciudad de Guayaquil, con la finalidad de validar que la propuesta de la implementación del Estándar PCI-DSS es una media que le permitirá a la institución mejorar la seguridad en las transacciones efectuadas con tarjetas de pago, con los resultados de este análisis y la información recolectada se confirmará que estándar ofrece una solución efectiva para incrementar el nivel de seguridad de la información sensible de las instituciones Bancarias.

PALABRAS CLAVES: Implementación, Seguridad de información, Tarjeta de Pago, PCI- DSS, institución financiera, Confidencialidad, requerimientos.

ABSTRACT

This paper proposes the analysis of the implementation of the Payment Card Industry Data Security Standard (PCI-DSS), as a security method to prevent fraud transactions involving the use of credit and debit cards, and as an aid to compliance with the requirements of the Superintendency of Banks and Insurance (Superintendencia de Bancos y Seguros SBS) regarding the processing of them.

This standard requires maximum data security for cardholder or owner of the card, so the idea of implementing PCI-DSS is for protecting and safeguarding sensitive and confidential information, allowing to financial institutions (banks, cooperative and other service providers) to ensure the security of customer data. The approach of this paper refers to the analysis of the implementation of PCI-DSS in a Bank located in the city of Guayaquil.

The analysis of the implementation of the PCI DSS standard covers from definition, functionality, requirements and components that integrate the identification of the best security practices that should apply the Bank.

On this analysis we take study about security mechanisms that has determined bank located in the city of Guayaquil, in order to validate that the proposed implementation of PCI-DSS is a way that will allow institution improve security in transactions with payment cards, with the results of this analysis and the information collected will be confirmed which standard t offers an effective solution to increase the level of security of sensitive and confidential information from banking institutions.

KEYWORDS: Implementation, Information Security, Payment Card, PCI-DSS, financial institution, Confidentiality, requirements.

INTRODUCCIÓN

El documento producto de esta investigación comprende el análisis de la implementación del estándar de Seguridad de Datos para la Industria de Tarjeta de Pago como una propuesta para reforzar la seguridad de información y garantizar el correcto procesamiento de tarjetas de crédito y débito dentro de un banco.

El objetivo de este análisis es demostrar la importancia de la implementación del estándar, definiendo la estructura del mismo, y detallando la garantía que proporciona sobre los datos del titular de la tarjeta.

En el **Capítulo I** se describen los puntos preliminares, se formula y detalla la problemática del proyecto, se plantean objetivos, se estipula la justificación del mismo.

En el **Capítulo II** se establece el marco teórico donde se describe la estructura del estándar PCI-DSS, dando a conocer cada uno de los requisitos necesarios para su implementación, y se detalla el tipo de información que debe protegerse.

En el **Capítulo III** se establece el marco metodológico, se detalla el tipo de investigación, se define el tipo de método investigativo empleado, se delimita la población, y se detallan las técnicas aplicadas para la recolección de datos.

En el **Capítulo IV** se analizan e interpretan los resultados de la información recolectada en las encuestas realizadas a la población seleccionada.

En el **Capítulo V** se definen conclusiones en base al desarrollo del proyecto y se plantean recomendaciones de acuerdo a los resultados obtenidos.

En el **Capítulo VI** se plantea la propuesta del proyecto como solución a la institución.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Enunciado del Problema

En la actualidad el avance tecnológico le ha permitido a las instituciones financieras brindar nuevos servicios bancarios, como es el caso de la banca en línea, y la banca móvil permitiéndoles a sus clientes realizar transacciones y consultas a través de Internet. Sin embargo a la par de los servicios, también incrementa la delincuencia (Cyberdelitos), dado que esta última se encarga de desarrollar nuevas tecnologías para realizar robos y estafas.

Entonces se puede decir que en la actualidad, es una obligación para los bancos desarrollar sistemas de protección sobre toda la información sensible y confidencial que posee de sus clientes, los cuales pueden acceder a ella por distintos canales de comunicación.

De los anteriores párrafos se desprende que servicios agregados de los bancos, tales como banca electrónica, banca móvil, compras online, entre otros, implican el manejo de dinero electrónico siendo por lo tanto común el uso de tarjetas de crédito y débito, que le permiten al cliente llevar a cabo su capacidad adquisitiva, sin tener el dinero físico con él. Estas transacciones involucran entonces un estrecho vínculo entre los sistemas de seguridad, la información del cliente y la protección que el banco debe generar en sus sistemas financieros.

1.2 Formulación del problema

Los fraudes más comunes están relacionados con las claves de banca electrónica y la clonación de tarjetas de crédito y débito de los clientes; con estas dos, los delincuentes generalmente realizan transferencias, pueden realizar retiros en efectivo o comprar

artículos de fácil venta. ¿Está el banco preparado para responder a sus clientes ante un fraude de este tipo y de qué forma afectaría esto a la imagen de la Institución?

Debido a lo importante que es proteger de la información sensible del dueño de una tarjeta o tarjetahabiente se debe implementar dentro del banco un estándar de seguridad robusto que proteja la información sensible ¿Tiene el banco implementado un estándar o norma que garantice la seguridad de información?, ¿Cuál es el riesgo que afrontaría por no tener implementado un estándar de seguridad? Bajo las interrogantes aquí expuestas se propone la implementación del estándar PCI-DSS (Payment Card Industry Data Security Standard), el cual proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los tarjetahabientes.

1.3 Objetivos

1.3.1 Objetivo General:

Demostrar la importancia de la implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS por sus siglas en inglés), los requerimientos que implica la Certificación del mismo dentro de un banco y la forma en que la aplicación del mismo beneficia a la institución.

1.3.2 Objetivos Específicos:

- Describir los requerimientos que exige el estándar de Seguridad de Datos para la industria de tarjetas de pago.
- Evaluar el grado de conocimiento del personal de los bancos respecto al estándar PCI-DSS.
- Descubrir qué porcentaje de las Instituciones Financieras encuestadas, cuentan con el estándar PCI-DSS.
- Determinar los cambios que se deben realizar en la organización para aplicar PCI-DSS.
- Validar el beneficio en la seguridad de la información de la empresa,

con la aplicación del estándar.

- Determinar el conocimiento del personal de seguridad de información del tiempo que le tomaría al banco, en el caso que no tenga el estándar, el proceso de implementación del mismo.
- Identificar el porcentaje de aceptación del estándar PCI-DSS, en cada una de las instituciones encuestadas.

1.4 Justificación

Este análisis surge con la necesidad de demostrar la importancia de realizar un estudio (muestreo) de la preparación que las instituciones bancarias deben cumplir previo a la implementación del estándar PCI-DSS.

En el mercado Bancario dentro de la sección de seguridad de la información para las industrias de tarjetas de pago, PCI Security Standars Concuil ofrece los estándares PA–DSS (Payment Applications vendors - Data Security Standard), PCI –PTS (Payment Card Industry – Pin Transaction Security), y PCI-DSS (Payment Card Industry), este último para empresas que realicen transacciones que impliquen el uso de tarjetas de pago.

Aplicar el estándar PCI-DSS le permite a todas instituciones financieras, haciendo énfasis a la banca, reducir el fraude relacionado con las tarjetas de crédito e incrementar la seguridad, lo que brinda confiablidad y continuidad al negocio, dado que por lo general los tarjetahabientes demandan que el banco al que le confían su dinero, sea líder en seguridad de tal forma que sus finanzas no se vean afectadas o comprometidas.

Las instituciones que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o de lo contrario se arriesgarían a perder sus permisos para procesar las tarjetas de crédito y débito.

Con este estudio se demostrará la importancia de la implementación del mencionado estándar dentro de un banco en el Ecuador, además que ayudará a tener una idea clara respecto al procedimiento de implementación del mismo. Los resultados que se adquieran con este análisis otorgarán un beneficio personal al poder ampliar conocimientos con respecto a las seguridades que se manejan actualmente en el sistema financiero en el Ecuador y la preparación de los empleados en los puntos clave de seguridad que deben cumplir para el mejor desempeño de sus funciones.

CAPITULO II

MARCO REFERENCIAL DE LA INVESTIGACIÓN

2.1 Marco Teórico

En este capítulo se presentarán los lineamientos teóricos para el análisis de la implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS sus siglas en su idioma nativo ingles) Versión 2.0, el cual tiene como objetivo principal mejorar el nivel de seguridad que promueve un entorno seguro de pago permitiendo encontrar una solución que satisfaga el escenario expuesto en la hipótesis.

Por otra parte se revisaran los conceptos relacionados al Estándar de Seguridad de la información, el mismo Estándar evalúa las vulnerabilidades del entorno y como resultado, para clasificar las vulnerabilidades se resaltan los beneficios puntuales que brinda dicho estándar: garantiza la protección de la información de los titulares de las tarjetas, minimiza el riesgo de posibles intrusiones no autorizadas, Incrementa la confianza de los tarjetahabientes y luchar contra la suplantación u otros fraudes, los cuales provocan la inseguridad del tarjetahabiente.

De igual manera, se explicarán los 12 requisitos del Estándar PCI-DSS, lo cual permite constatar los beneficios antes mencionados, que son fundamentales para lograr la certificación con el fin de que los tarjetahabientes confíen en la institución a la cual le están confiando su información sensible.

2.2 Marco Conceptual

Se puede resumir que la iniciativa principal de Payment Card Industries Security Standars Council (PCI-SSC), entidad reguladora creada en septiembre 7 del 2006 y conformada por American Express, Discover Financial Services, MasterCard

Worldwide, Visa Inc. y JCB international, que se asociaron para crear un nivel de protección adicional, es decir, tratar de mantener una norma de Seguridad global la que permita mejorar la seguridad de los datos del tarjetahabiente. Este estándar es de cumplimiento obligatorio, la finalidad de PCI-DSS es reducir el fraude relacionado con tarjetas de pago.

Visto de esta forma las normas de seguridad de PCI en efecto son requisitos técnicos y operacionales, los cuales son establecidos por el Consejo de Normas de Seguridad de la Industria de Pagos (PCI-SSC) para proteger los datos confidenciales del titular de la tarjeta.

Evidentemente las normas se rigen a nivel mundial. De este modo el estándar garantiza la existencia de un marco global consistente para la protección de los datos de cuentas bancarias, tarjetas, transacciones y datos de autenticación. Es por ello que se aplica a las entidades que participan en los procesos de las tarjetas de pago (comerciantes, instituciones financieras, entidades adquirentes, entidades emisoras, proveedores de servicios y otros) y en general, a toda organización que almacene, procese o transmita datos de cuentas, siendo el número de cuenta (Primary Account Number, PAN) el factor que determina la aplicabilidad.

Por consiguiente el estándar incluye los requisitos mencionados a continuación: Administración de Seguridad, Arquitectura de Redes, Diseño de Software, Políticas, Procedimientos y otras medidas de protección para ayudar a las organizaciones a proteger los datos de las cuentas del cliente en forma proactiva. Es importante mencionar que para poder obtener la certificación se debe cumplir con los requisitos mencionados.

En la actualidad, PCI-DSS es gestionado, revisado y actualizado por el PCI Security Standards Council.

2.2.1 Alcance de la evaluación del cumplimiento de los requisitos de las normas PCI-DSS

Debe señalarse que el primer paso de una evaluación PCI-DSS es determinar con exactitud el alcance de la revisión. Dicho de otro modo la entidad evaluada debería identificar todas las ubicaciones y flujos de datos de titulares de tarjetas antes de la evaluación anual, para lo cual realiza lo siguiente: La entidad evaluada identifica y documenta la existencia de todos los datos del tarjetahabiente, a fin de que pueda verificar que no haya datos fuera del entorno actual.

Se debe considerar que una vez que se hayan identificado y documentado todas las ubicaciones de los datos de los tarjetahabientes, la entidad utiliza los resultados para verificar que el alcance de las PCI-DSS sea apropiado.

Para poder determinar si afecta PCI-DSS a la institución es necesario iniciar una evaluación la cual permita conocer como los datos de titulares de tarjetas de pago fluyen a través de la institución, esto permitirá analizar lugares críticos ya sean estos en el almacenamiento, procesamiento o tratamiento de la información, eliminando flujos que no sean críticos. Es necesario que se evalúe cada uno de los flujos, donde hayan datos de tarjetas de pago, por ende se considera el punto inicial (qué, cuándo y cómo llegan los datos de tarjetas a la institución), los puntos intermedios (todos los sistemas y ubicaciones por los que fluyen los datos) y el punto final (si existe, cómo salen de la institución los datos).

Mediante este análisis, el cual se debe llevar a cabo en todas las áreas de la institución o compañía, es tan común que por lo general un área de la institución desconozca qué otras áreas también interactúan con datos de tarjetas de pago.

A continuación, se mencionan algunos ejemplos de flujos o servicios en los que pueden aparecer datos de tarjetas de pago en algún instante durante el análisis:

- Procesado, almacenado o transmisión de transacciones de pago.

- Proveedores de servicio (cualquier servicio ofrecido sobre el cual se pueda transmitir, almacenar o procesar datos de tarjetas por parte del proveedor de servicio o del propio cliente); como:
    - ✓ Alojamiento de espacios web, servidores dedicados, Housing, Datacenter.
    - ✓ Servicios de red, administración y gestión de sistemas.
    - ✓ Desarrollo de aplicaciones.
- Facturación/pago de servicios mediante tarjeta por internet, teléfono, móvil, etc.
- Servicios de atención al cliente donde aparezcan datos de tarjetas, por ejemplo:
    - ✓ Call-centers (conversaciones grabadas).
    - ✓ Incidencias recibidas en papel, por ejemplo fax.
    - ✓ Incidencias recibidas electrónicamente (correo electrónico, aplicaciones, etc.).
- Hospedaje y/o gestión de servicios de clientes que contengan datos de tarjetas de pago.
    - ✓ Programas de lealtad.
    - ✓ Gestión de fraude con datos de tarjetas.
    - ✓ Gestión de reservas.

Una vez que ya se hayan identificados los flujos de datos, es de suma importancia buscar las áreas donde se pueda fortalecer los datos de las tarjetas de pago o eliminarlos.

Con la información obtenida se podrá determinar el alcance de PCI-DSS, tomando en cuenta que si algún otro sistema se encuentra en la misma zona de Red de los componentes identificados en el flujo de los datos, también estará dentro del alcance de PCI-DSS aunque no forme parte en la gestión de los datos de titulares de tarjetas.

2.2.2 Segmentación de red

Una adecuada segmentación de red permite a las instituciones reducir el alcance y el coste de la adecuación y evaluación del Estándar, teniendo como objetivo principal delimitar los sistemas que permiten que los datos de las tarjetas de pago sean procesados, almacenados y transmitidos, logrando así limitar el alcance de PCI que es lo ideal.

La intención es proteger los datos contra amenazas de otras redes o entornos que podrían afectar a los datos de tarjetas de pago. Para ello es necesario evaluar posibles interacciones entre un entorno PCI-DSS y otro entorno, como por ejemplo una red de gestión de un proveedor de servicios.

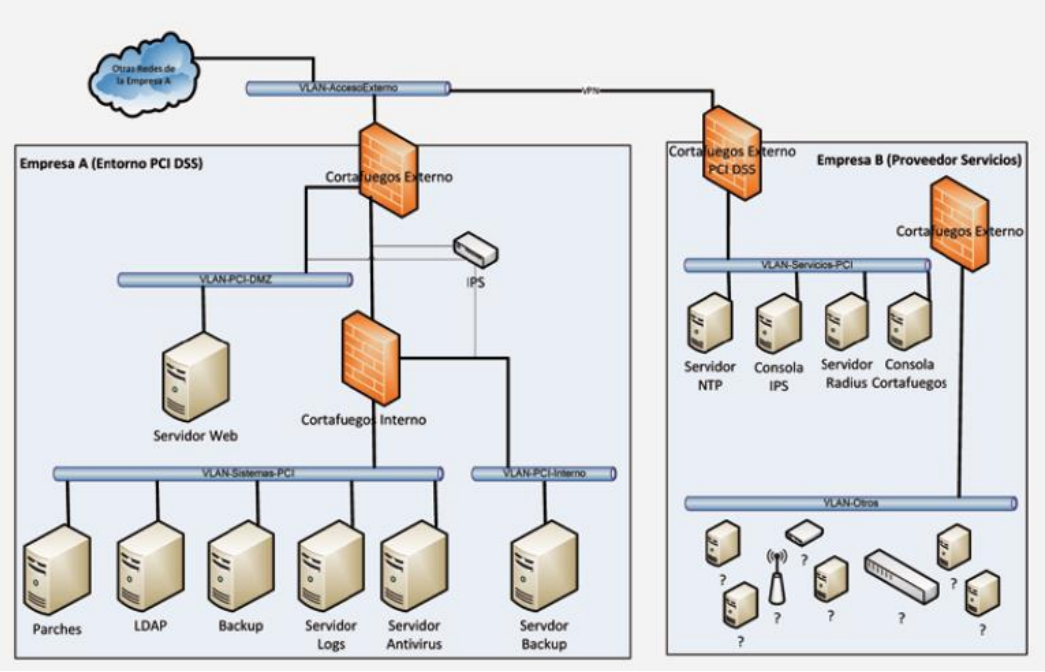


Figura 1. Segmentación de Red.
Fuente: Internet Security Auditors

2.2.3 Importancia de la Segmentación de Red

Sin una adecuada protección de red, todos los elementos conectados a los componentes donde se procesan, transmiten o almacenen datos estarían afectados, ya que las redes simples dejan todos los sistemas vulnerables lo cual incrementan las posibilidades de violación de los datos, esto puede ocurrir en cualquier comercio o sitios que acepten tarjetas de pago. Si un intruso "hacker" consigue el acceso a través del punto más débil de la red puede alcanzar otros sistemas críticos en otras ubicaciones.

Por otra parte se debe tener bien en claro que la segmentación de red no es un requerimiento obligatorio de PCI-DSS, pero una red mal segmentada, errónea o incompleta, aumenta el riesgo en la organización, dificultando al momento de implementar y mantener los controles de PCI-DSS. A mayor riesgo mayor deberá ser el control.

Por ello es de gran importancia realizar un control más exhaustivo realizando test de intrusión de red y aplicación, escaneos de vulnerabilidades internos y externos, registros de auditorías y logs estrictos, configurar de modo seguro todos los componentes, utilizar cortafuegos o firewalls como seguridad para aplicaciones que no tienen relación con los datos de tarjeta de pago, y gestionar las políticas de seguridad para todos los componentes de la red.

2.2.4 Pautas reglamentarias para una Segmentación correcta

La Norma de Seguridad PCI-DSS proporciona una orientación clara sobre la separación de los datos dentro de la red, es decir en el caso del PCI, los datos de titulares de tarjetas serán aislados del resto de la red, ya que contiene información muy sensible.

Un ejemplo claro sería asegurar que el *Punto de Venta de sistemas y bases de datos* (POS) debe estar separado de las zonas de la red a la que tengan acceso personas ajenas, en una Zona PCI se crean limitaciones estrictas las cuales permiten la

conectividad para un número reducido de servidores y aplicaciones posibles. (Blaustein, 2014)

2.2.5 Rutas que permiten una segmentación adecuada

Es muy importante tener en cuenta que los firewalls y las VLANs proporcionan una ruta la cual permite dividir la red en zonas; al permitir que se divida la red en zonas se están imponiendo un conjunto de reglas que controla las rutas de comunicación.

Tener una excelente política de seguridad implica que la segmentación de la red será dividida en varias zonas; con la aplicación de una política de seguridad rigurosa le permite pasar de una zona a otra. Todo lo que se asigne en la zona de PCI, debe ser aislado del resto de la red.

Los últimos casos de violación de información a través de la red demostraron que una mala segmentación de la red aumenta significativamente el robo de información o la interrupción del Sistema. Por lo general las redes planas son simples y no necesitan muchos gastos de gestión, por lo que realmente necesitan una protección adecuada. (Blaustein, 2014)

2.2.6 Beneficios de reducir el alcance del entorno de los datos del titular de la tarjeta dentro de una organización

Segmentar el entorno de datos de tarjetas de pago permite reducir significativamente el alcance que debe cubrir PCI-DSS. A continuación se puede describir algunos elementos que pueden verse reducidos si la red está debidamente segmentada:

- Reducir el alcance del acceso a los datos, es decir que solo el personal autorizado pueda acceder al entorno de datos de tarjetas de pago.
- Número de sistemas (servidores, aplicaciones, dispositivos).

- Menor esfuerzo para desarrollar y aplicar políticas de seguridad.
- Menor coste, por ejemplo al realizar una auditoría en caso que se tenga menores componentes, su costo será menor.
- Menor esfuerzo forense, por ejemplo en el caso de que ocurra algún incidente de seguridad, al realizar una investigación forense en un segmento de red limitado es mucho más rápida y efectiva.

Un *Asesor de Seguridad Calificado* (QSA) puede ayudar a determinar el alcance del entorno de datos de los titulares de tarjetas de una entidad; además de proporcionar orientación sobre cómo reducir el alcance de una evaluación de las PCI-DSS al implementar una segmentación apropiada de la red. (COUNCIL, PCI SECURITY, 2010, pág. 5)

2.2.7 Tarjetas de Pago

Son medios de pago emitidos por una entidad financiera o un comercio. Debido a su comodidad y facilidad de uso así como su amplia aceptación y por la seguridad que supone no tener que llevar dinero en efectivo, las tarjetas se han convertido en complemento de vida actualmente.

Las tarjetas de Pago son el medio más aceptado para efectuar compras por internet, en viajes y desplazamientos. En la actualidad, una tarjeta de crédito es algo casi fundamental.

2.2.7.1 Elementos de datos de titulares de tarjetas y de datos confidenciales de autenticación

El Estándar define los datos de titulares de tarjetas y datos confidenciales de autenticación, como se detalla a continuación:

Tabla 1. Elementos de Datos de Titulares de Tarjetas y de Datos confidenciales de autenticación

Datos de los Tarjetahabientes	Datos confidenciales de autenticación
Número de cuenta principal (PAN) Nombre del titular Fecha de expiración Código de servicio	• Los datos completos de la pista (datos de banda magnética, o su equivalente en un chip) • Números CAV2/CVC2/CVV2/CID • Pins / bloqueos de PIN

Fuente: PCI Security Council

Los requisitos de las PCI-DSS se aplican si se almacena, procesa o transmite un número de cuenta principal (PAN).

Si un PAN no se almacena, ni se procesa ni se transmite, no se aplican los requisitos de las PCI-DSS.

En caso de que el nombre del tarjetahabiente, el código de servicio o la fecha de vencimiento, no se almacenan ni procesan ni transmiten con el PAN, ni están presentes de alguna u otra manera en el entorno de datos del titular de la tarjeta, se deben proteger de acuerdo con todos los requisitos de las normas PCI-DSS.

Las normas PCI-DSS representan un conjunto mínimo de objetivos de control que puede ser reforzado con leyes y regulaciones locales, regionales y sectoriales. Además, la legislación o las regulaciones pueden requerir protección específica de la información de identificación personal u otros elementos. (COUNCIL, PCI SECURITY, 2010, pág. 6).

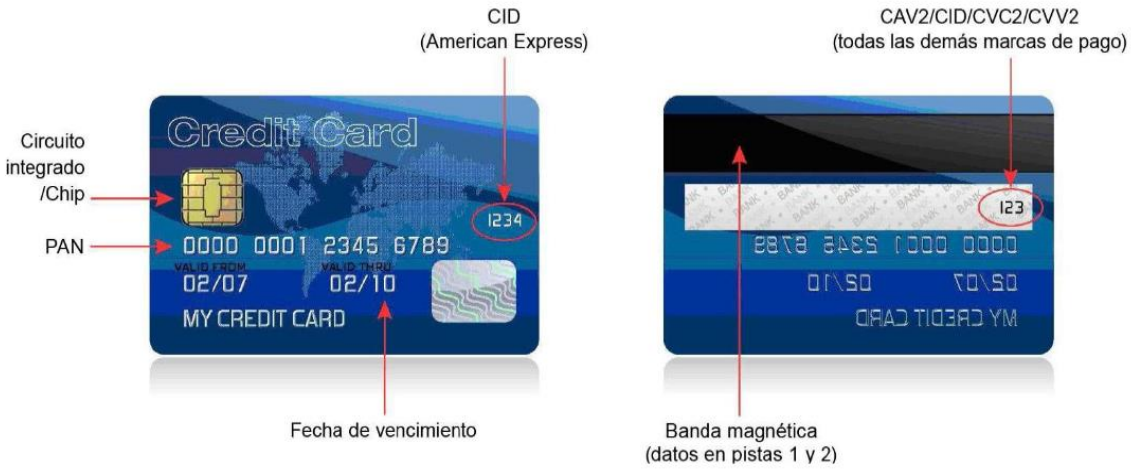
2.2.7.2 Ubicación de datos de titulares de tarjetas y de datos confidenciales de autenticación

Los datos confidenciales de autenticación constan de los datos de la banda magnética (o pista), código o valor de validación de la tarjeta, y datos del PIN.

¡Se prohíbe el almacenamiento de datos confidenciales de autenticación después de la autorización! (PCI Security Council, 2013, pág. 37)

Estos datos son muy valiosos para las personas malintencionadas, ya que le permite generar tarjetas de pago falsas y crear transacciones fraudulentas. La **Figura 2** muestra el frente y el reverso de una tarjeta de crédito en la cual se muestra la ubicación de los datos del titular de la tarjeta y los datos confidenciales de autenticación. (COUNCIL, PCI SECURITY, 2010, pág. 8).

Figura 2. Ubicación de los Datos de los Titulares de Tarjetas.



Fuente: PCI Security Council

- **PAN (Primary Account Number)**

Debido a la gran necesidad de establecer un medio de pago común en los comercios y ante la gran demanda de las tarjetas de crédito o débito como método de pago a nivel local e internacional, surgió la necesidad de permitir el intercambio de información entre las diferentes entidades involucradas.

Las instituciones financieras comenzaron a buscar asociaciones ubicadas en los distintos lugares las cuales permitan realizar los pagos con sus tarjetas, dando así la facilidad al cliente. La idea empezó a dar frutos para lo cual optaron por gestionar entre los bancos asociados, un número de cuenta compartido, de tal manera que un cliente que tenga sus servicios podría hacer uso de dicho número en cualquiera de los bancos afiliados sin ningún problema, Luego surgieron organizaciones como VISA, MasterCard, American Express, JCB y Discover (entre otras), las cuales permitían transacciones interbancarias entre los asociados.

Debido a todo lo anteriormente dicho el número de cuenta interbancario recibió el nombre de **PAN** (Primary Account Number), el mismo que viene impreso y estampado en altorrelieve en los plásticos de las tarjetas de pago.

- **Esquema de numeración del PAN (Primary Account Number)**

Para permitir operatividad entre los diferentes tipos y marcas de tarjetas, la ISO (International Organization for Standardization) publicó el estándar ISO/IEC 7812 "Identification cards — Identification of issuers" que establece una serie de criterios que permiten la interoperabilidad de los PAN (Primary Account Number), tanto en comercios como en proveedores de servicios y bancos adquirientes. A continuación se observa en la Figura el esquema de la numeración PAN: (7812-2:2007, ISO/IEC)

Figura 3. Esquema de la Numeración PAN.

Fuente: ISACA

A continuación se explicara cada uno de los dígitos con su esquematización:

- ✓ **Major Industry Identifier (MII)**

  Es el primer dígito del PAN, identifica el tipo de sistema al que la tarjeta está asociada:

  1) 0: ISO/TC 68 y otros.

  2) 1: Aerolíneas.

  3) 2: Aerolíneas y otros.

  4) 3: Viajes, entretenimiento y finanzas (American Express, JCB y Diners Club).

  5) 4: Banca y finanzas (VISA).

  6) 5: Banca y finanzas (MasterCard).

  7) 6: Mercadeo y banca/finanzas (Discover).

  8) 7: Empresas petroleras y otros.

  9) 8: Salud, telecomunicaciones y otros.

  10) 9: Asignaciones futuras.

- ✓ **Issuer Identifier Number (IIN) o Bank Identification Number (BIN):**

  Está compuesto por los seis primeros dígitos de la tarjeta (incluyendo el MII). El cual permite la identificación del banco emisor de la tarjeta para el respectivo enrutamiento de transacciones interbancarias. En la actualidad es gestionado por American National Standards Institute (ANSI).

- ✓ **Individual Account Identification (IAI):**

  El número está compuesto por los dígitos a partir del séptimo hasta el penúltimo, permite identificar el número de cuenta asociado al titular de tarjeta.

- ✓ **Check Digit:**

  Es el último dígito de la tarjeta y es calculado usando el algoritmo de Luhn (Es una fórmula de suma de verificación, utilizada para validar una diversidad de números de identificación).

  Muchas veces la longitud del PAN depende de la marca de tarjetas que lo gestiona y del área de emisión:

  1) Visa y Visa Electron: 13 o 16 dígitos.

  2) Mastercard: 16 dígitos.

  3) Discover: 16 dígitos.

  4) American Express: 15 dígitos.

  5) Diners Club: 14 dígitos.

  6) Maestro: 12 a 19 dígitos (para tarjetas débito internacionales).

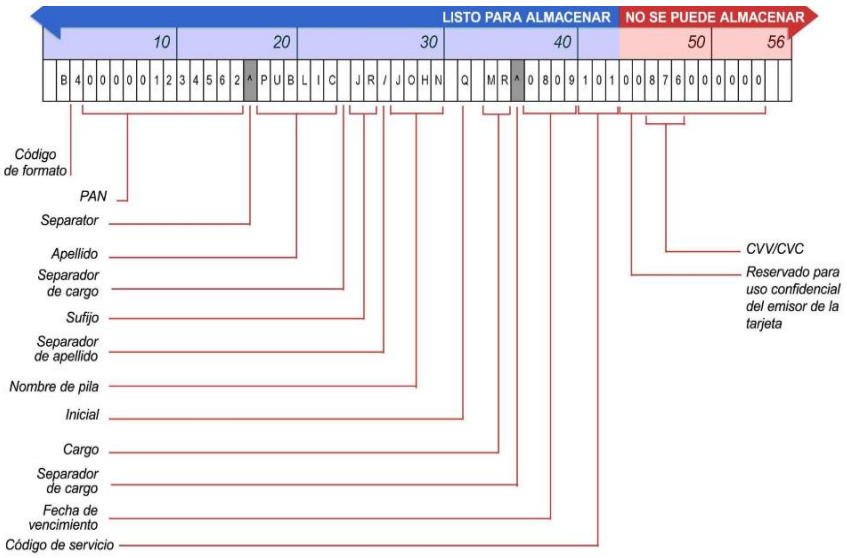
  7) JCB: 15 o 16 dígitos (para Japón).

- **Datos de la Banda Magnética: Comparación de la Pista 1 vs. Pista 2**

Pista 1.

- ✓ Contiene todos los campos de la pista 1 y la pista 2.
- ✓ Longitud de hasta 79 caracteres

Figura 4. Datos de la Pista 1.

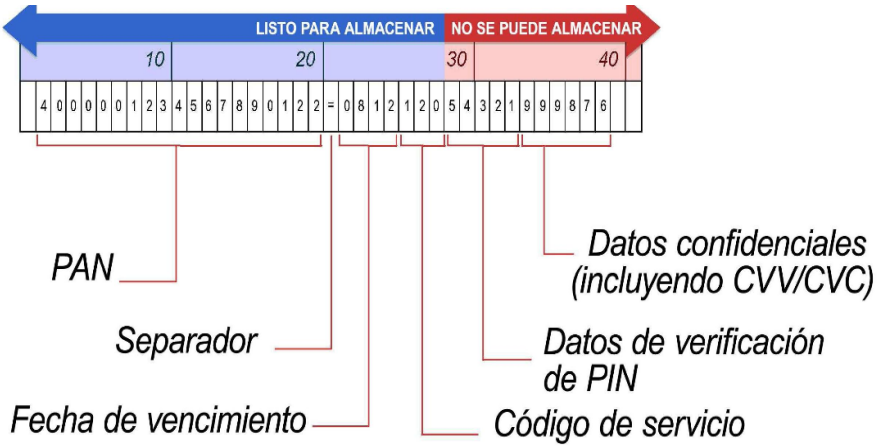


Fuente: ISACA

Pista 2.

- ✓ Menor tiempo de procesamiento en el caso de transmisiones de dial-up anteriores.
- ✓ Longitud de hasta 40 caracteres.

Figura 5. Datos de la Pista 2.



Fuente: ISACA

- **El número CVV (" Card Verificaction Value, Valor de Verificación de la Tarjeta ")**

  Las tarjetas de crédito o tarjetas de débito tienen un CVV, en el caso de las marcas de tarjetas VISA, MasterCard y Discover tienen un número de 3 dígitos. La tarjeta de crédito o débito de marca American Express tienen un código numérico de 4 dígitos.

Figura 6. El CVV en las Tarjetas de Pago.

Fuente: Artelista

Los números PIN (Numero Personal de Identificación) permiten usar su tarjeta de crédito o débito en un cajero automático o realizar una compra en persona con su tarjeta de débito o un adelanto en efectivo con cualquier tarjeta de crédito.

Los números CVV no son el número secreto (Clave PIN) de su tarjeta.

Los números CVV también se los conoce como números de CSC ("Código de seguridad de la tarjeta"), los números CVV2, son los mismos que los números CVV, con una pequeña excepción, que éstos han sido generados por un proceso que dificulta adivinar el número en caso de clonación de las tarjetas.

2.2.8 Requisitos de la Norma de Seguridad PCI – DSS.

El consejo categoriza las normas en 12 requerimientos de "alto nivel", los cuales se describen a continuación, y cada requisito contiene sub-requisitos técnicos que las empresas deben revisar cuidadosamente. (COUNCIL, PCI SECURITY, 2010)

2.2.8.1 DESARROLLAR Y MANTENER UNA RED SEGURA.

1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.

Este requisito hace referencia a la protección de los datos para lo cual es necesario instalar y mantener la configuración del firewall, es por ello que una forma de hacerlo es revisando la estructura de la red y la configuración del firewall y otros sistemas de red, es vital documentar todas las configuraciones y cambios realizados.

2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

En este requisito hace referencia a la necesidad de no utilizar opciones por defecto en contraseñas y valores de configuración. En base a aquello, se revisaran los sistemas operativos, los servicios de red, los dispositivos de red y filtrado en busca de las configuraciones, ficheros, usuarios y contraseñas, etc., en efecto se darán soluciones seguras.

2.2.8.2 PROTEGER LOS DATOS DEL TITULAR DE LA TARJETA.

3. Proteger los datos del titular de las tarjetas que fueron almacenados.

Para lograr una protección segura de los datos, es necesario analizar las políticas y procedimientos de seguridad, el cumplimiento legal vigente y las normas de retención y destrucción de los datos de tarjetas. De esta manera, es preciso asegurar que no se almacene ningún tipo de información relativa en las mismas, para ello se emplean métodos realmente válidos de encriptación de información y claves.

4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

Este Requisito se refiere a las transmisiones de información Confidencial la cual debe ser Cifrada durante la transmisión a través de redes públicas a las cuales pueden acceder fácilmente los delincuentes.

2.2.8.3 MANTENER UN PROGRAMA DE ADMINISTRACIÓN DE VULNERABILIDAD.

5. Utilizar y actualizar con regularidad los programas o software anti-virus.

Se utiliza software antivirus adecuado en los puntos apropiados de la red ya que el estándar lo impone, para ello también se realiza actualización periódica y adecuada de este software.

6. Desarrollar y mantener sistemas y aplicaciones seguras.

Hace referencia al desarrollo y mantenimiento de sistemas y aplicaciones seguras, toda organización debe repasar sus políticas de actualización. En menos de 30 días debe la aplicación asegurar sus parches críticos, evidenciar que disponen de las herramientas y procedimientos apropiados para la identificación de vulnerabilidades, evidenciar que cuentan con entornos de desarrollo y de producción separados, la información y las medidas de seguridad adecuadas; finalmente, asegurarse de que en el desarrollo de las aplicaciones no aparecen vulnerabilidades documentadas.

2.2.8.4 IMPLEMENTAR MEDIDAS SOLIDAS 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.**

En este punto se establece el acceso restringido a los datos importantes, es decir asegurar que solo el personal autorizado pueda acceder a ellos conforme a la necesidad de conocer y a la responsabilidad del cargo. Por consiguiente, se revisara la política de seguridad en busca de la definición de los controles de acceso para todos los sistemas, aplicaciones e información.

8. **Asignar una ID exclusiva a cada persona que tenga acceso por computadora.**

La Asignación de un ID único a cada persona con acceso a los sistemas, para ello es necesario verificar que la persona tenga un único ID, el cual le permita acceder a los datos, no puede existir duplicidad de ID, previo a eso debe existir un proceso de encriptación de ID y auditar la asignación de ID.

9. **Restringir el acceso físico a los datos del titular de tarjeta.**

Para restringir el acceso físico a los datos, se crea la posibilidad de rastrear las actividades del usuario, con unos sistemas de control de acceso el cual permite el rastreo, alerta y análisis cuando algo no va bien; sin registros de actividades del Sistema es muy difícil encontrar la causa de algún riesgo.

2.2.8.5 SUPERVISAR Y EVALUAR LAS REDES CON REGULARIDAD.

10. **Rastrear y supervisar todos los accesos a los recursos de Red y datos de los titulares de las tarjetas.**

En este requisito se audita y monitorea todos los accesos a la red (Recursos) y los datos de usuarios, tiene que ver con los registros de actividad del sistema.

11. **Probar periódicamente los sistemas y procesos de seguridad.**

En este punto se auditará la seguridad de los sistemas y procesos, en efecto se asegura el escaneo de vulnerabilidades de forma regular, es necesario revisar los procedimientos de búsqueda de puntos peligrosos.

2.2.8.6 MANTENER UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

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

Se refiere al mantenimiento de una política la cual permita que se gestione la seguridad de la información, para lo cual se debe comprobar los procedimientos del accionar diario con la finalidad de buscar deficiencias en la documentación, también se revisa la documentación de los procedimientos de gestión de incidentes en la empresa.

Finalmente es necesario tener en cuenta que para brindar Seguridad a los Tarjetahabientes las Instituciones Financieras deben cumplir con el estándar de Seguridad PCI-DSS, para lograr la certificación deben cumplir una serie de requisitos de Seguridad. Esto se consigue estableciendo y manteniendo un sistema de seguridad de datos, protegiendo la información de los titulares de las tarjetas, mejorando los programas de gestión de datos, implementando fuertes medidas de control de la seguridad, analizando y estudiando las incidencias que surgen y, sobre todo, asegurando el correcto uso de las políticas de seguridad de la información.

Para mayor información referente a los Requisitos y ahondar más el tema puede revisar el documento "Norma de seguridad de datos de la Industria de tarjetas de pago (PCI)", cual se encuentra en la página oficial de PCI Security Council.

Durante el desarrollo del presente documento surgió una versión mejorada del Estándar PCI-DSS que es la versión 3.0, la cual incluye una nueva sección que

proporciona recomendaciones para la implementación de cada una de las directrices de seguridad en las actividades de "business-as-usual" de una empresa.

Las normas ayudan a garantizar que las empresas encargadas de transmitir, procesar y almacenar la información de las tarjetas de pago se encuentren protegiendo adecuadamente a los datos del tarjetahabiente y la protección contra las violaciones de datos. Las normas pueden exigir que las empresas deban modificar las políticas de seguridad actuales.

Las empresas que no cumplan con las normas establecidas por PCI-DSS pueden enfrentar multas si llegase a existir una violación de datos, demandas colectivas, informes de auditoría negativos, y la crítica del público, lo cual deja en mal prestigio a la empresa.

Por ello en caso de que no se cumpliera con la norma, las marcas de tarjetas con quienes se opere pueden imponer sanciones o multas, llegando, incluso, a la denegación del servicio de utilización de sus tarjetas. (PCI Security Council, 2013)

La nueva versión aclara los requisitos existentes y añade requisitos técnicos adicionales que incluyen:

1. Asegurar que las soluciones anti-virus se están ejecutando de forma activa y no se pueden desactivar o ser alterados por los usuarios.

2. La evaluación de la evolución de las amenazas de malware para sistemas no considerados como comúnmente afectados por software malicioso.

3. La implementación de prácticas de codificación que protegen contra autenticación y gestión de sesiones.

4. La implementación de una metodología para las pruebas de penetración (el 1 de julio de 2015).

5. Exigir a los proveedores de servicio con acceso remoto, utilizar las credenciales de autenticación única para cada cliente.

6. Exigir que los mecanismos de autenticación, tales como Tokes de seguridad o tarjetas inteligentes, estén vinculados a una cuenta individual.

7. El control del acceso físico a las áreas sensibles para el personal en sitio.

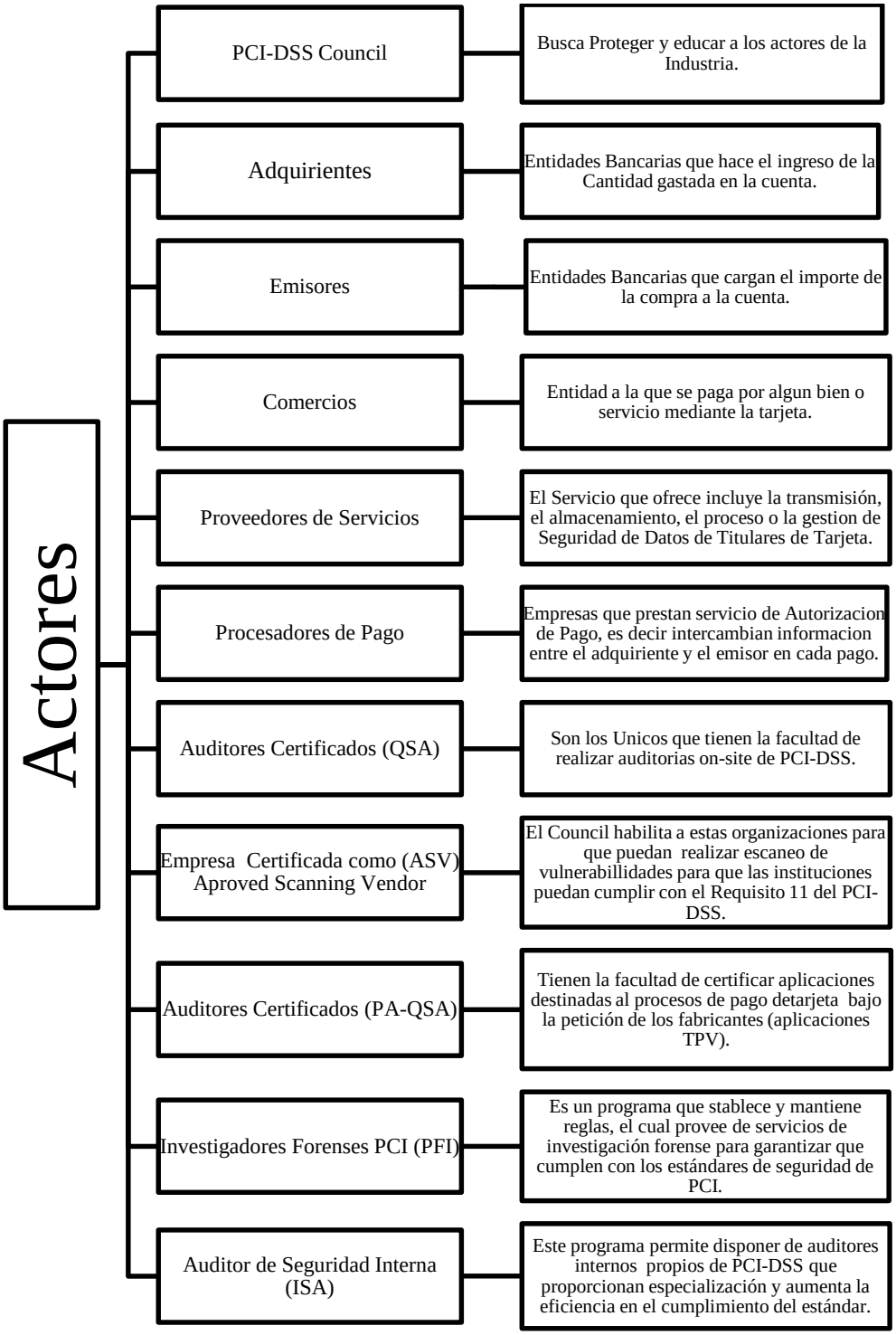
8. Fortalecimiento de la seguridad de contraseñas.

9. El mantenimiento de cierta documentación, incluida la información acerca de qué requisitos de PCI-DSS son gestionados por la entidad y cuales requisitos son gestionados por los proveedores de servicios.

10. Exigir a los proveedores a reconocer por escrito a sus clientes de que es responsable de la seguridad de los datos de titulares de tarjetas que posee (el 1 de julio de 2015). (PCI Security Council, 2013) Versión 3.

2.2.9 Actores en PCI-DSS

A continuación se menciona todos actores que intervienen en la implementación del Estándar de Seguridad: (COUNCIL, PCI SECURITY, 2010)



Fuente: PCI-DSS Seguridades

Elaborado por: Autores

2.2.10 Riesgos y vulnerabilidades

2.2.10.1 Definición de Fraude

Por fraude se entiende la acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete. Acto cumplido intencionalmente tendiente a eludir, herir o menoscabar disposiciones legales o derechos del Estado o de terceros. Engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio. (Supertel, Fraudes en telecomunicaciones, 2008).

2.2.10.2 Fraudes Comunes

La delincuencia se desarrolla y se encarga de crear tecnología para fines inmorales, como lo son el robo y la estafa. Es por esto que tanto las instituciones financieras como sus clientes deben estar alerta a este tipo de riesgos. (Superintendencia de Bancos del Ecuador, 2012).

2.2.10.3 Los fraudes más conocidos son:

1. Fraudes relacionados con las claves de banca electrónica de los usuarios. Con estas claves, los delincuentes realizan transferencias de cuentas de clientes hacia otras personas y luego realizan retiros en efectivo.

2. Ofertas en página web de productos o servicios que no existen.

3. Suplantación de identidad, es decir que los delincuentes abren cuentas o realizan transacciones a nombre de las personas a las que les han robado su cédula o pasaporte. (Superintendencia de Bancos del Ecuador, 2012)

Formas de engañar a los usuarios para obtener claves.

Los delincuentes tienen diferentes formas de engañar a los usuarios para obtener claves, algunas de estas formas son:

Phishing:

Los delincuentes obtienen información confidencial a través de un correo electrónico en el que engañan al usuario haciéndole creer que debe enviar sus claves o datos para confirmación o actualización de datos.

Otra forma es suplantar la página web de la institución financiera, es decir, colocar otra página en su lugar, que se ve muy parecida. (Superintendencia de Bancos del Ecuador, 2012)

Phaming:

Similar al anterior, pero en esta modalidad el delincuente re-direcciona al usuario, es decir, lo manda a una página que se ve como la original de su banco y que recogerá las claves confidenciales cuando el usuario las digite. (Superintendencia de Bancos del Ecuador, 2012)

Malware:

El malware bancario, los troyanos y keyloggers son todos programas utilizados para fines delictivos, como por ejemplo aquellos diseñados para captar y grabar las teclas que el usuario digita cuando ingresa su clave en una página web. (Superintendencia de Bancos del Ecuador, 2012)

Skimming:

Al momento en que una persona entrega su tarjeta de crédito en un local comercial, el delincuente la pasa por un aparato llamado skimmer que graba la

información de la banda magnética de la tarjeta y luego la graba en una tarjeta falsa. (Superintendencia de Bancos del Ecuador, 2012)

Estafa Piramidal:

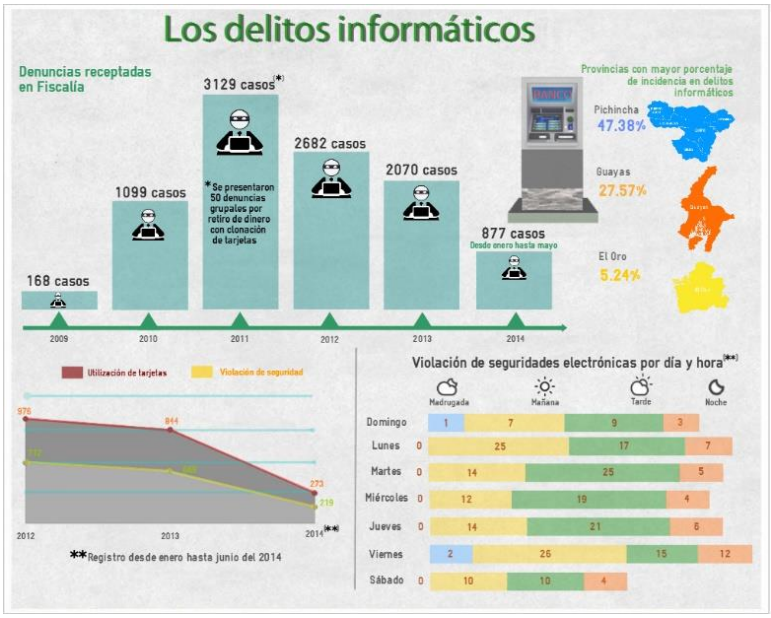
La estafa piramidal, el hoax y la carta nigeriana se distribuyen por correo electrónico y tratan de convencer al usuario de que entregando una suma de dinero o sus claves electrónicas, luego obtendrá grandes ganancias a través de una red social en la que aportan muchas personas. (Superintendencia de Bancos del Ecuador, 2012).

2.2.10.4 Ciberdelito

Es toda acción delictiva o ilícita en la que interviene el uso de un ordenador, software informático o medio de comunicación como internet, con el objeto de causar daño, robo, fraude o violación de la propiedad intelectual.

En la **figura 7** se puede observar que los Delitos informáticos en las provincias de mayor incidencia en los últimos 5 años han disminuidos gracias a que las Instituciones financieras decidieron aplicar normas de seguridad que protegen al tarjetahabiente (Datos del Clientes).

Figura 7. Delitos Informáticos.



Fuente: Diario el Ciudadano

2.2.10.5 Ciberseguridad

Es el conjunto de mecanismos de control de seguridad del entorno de una red, tales como políticas, software de protección, directrices, métodos de gestión de riesgos y vulnerabilidades que pueden emplearse para prevenir los delitos cibernéticos.

Precauciones que se deben tener en cuenta al momento de realizar transacciones con tarjeta desde un ATM.

La delincuencia emplea el uso de dispositivos que tienen características similares a los que posee un ATM o cajero automático, con la finalidad de obtener la información contenida dentro de la banda magnética de la tarjeta y la clave de autenticación de la misma.

Figura 8. Consejos de Cyberseguridad.

Fuente: EMOL

Consejos para el buen uso de Tarjetas de Débito y Crédito dirigido a los tarjetahabientes:

1. Tenga en cuenta que los bancos y entidades financieras no piden claves secretas de tarjetas, ni los nombres de sus familiares más cercanos por teléfono o correo electrónico. Esto podría ser un phishing. (Superintendencia de Bancos del Ecuador, 2012)
2. Apenas reciba su tarjeta, firme en la parte de atrás con tinta negra y recuerde que nadie podrá hacer compras fraudulentas con su tarjeta si comprueban su firma con la firma de su cédula. (Superintendencia de Bancos del Ecuador, 2012)
3. Nunca lleve con usted todas sus tarjetas.
4. Si sale de viaje, comuníquelo a su entidad financiera.
5. Si se cambia de dirección, igualmente notifíquelo.
6. Mantenga sus tarjetas en un lugar seguro.
7. Revise constantemente sus consumos para que pueda detectar cualquier irregularidad.
8. Nunca escriba su clave, memorícela y cámbiela cada cierto tiempo.
9. No realice transacciones vía internet desde computadoras públicas.
10. Nunca dé su clave o PIN a NADIE.
11. Cuando realice consumos con su tarjeta de crédito, esté pendiente de que no le realicen un "skimming" y revise que la tarjeta que le devuelven sea la suya.
12. Si va a realizar compras fuera de sus hábitos, comuníqueselo a la entidad financiera.
13. Lleve siempre el número de contacto de la tarjeta de crédito para reportar robos.
14. Guarde sus estados de cuenta.

15. Guarde los vales y recibos de sus tarjetas.

La Superintendencia de bancos y seguros tiene un Departamento de Servicio al Cliente (SAC) para recibir sus quejas y reclamos, y defender sus derechos frente a las instituciones controladas. (Superintendencia de Bancos del Ecuador, 2012)

2.3 Marco Legal

La Junta Bancaria del Ecuador JB-2012-2148, resuelve:

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero" de la Codificación de Resoluciones de la Superintendencia de bancos y seguros y de la Junta Bancaria, efectuar los siguientes cambios: (Superintendencia de Bancos del Ecuador, 2012)

ARTÍCULO 1.- En el capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de bancos y seguros", del título II "De la organización de las instituciones del sistema financiero privado", efectuar las siguientes reformas:

1. En el artículo 39, efectuar las siguientes reformas:

1.1 Sustituir el numeral 39.2, por el siguiente:

"39.2 Protección contra clonación de tarjetas.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;" (Superintendencia de Bancos del Ecuador, 2012)

ARTÍCULO 2.- En el capítulo V "De la gestión del riesgo operativo", del título X "De la gestión integral y control de riesgos", efectuar las siguientes reformas:

2. En el numeral 4.3.7. Sustituir el punto por punto y coma, e incluir los siguientes numerales:

4.3.8 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente:

4.3.8.1 Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;

4.3.8.2 Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información;

4.3.8.3 El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;

4.3.8.4 La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado;

4.3.8.6 Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;

4.3.8.8 Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad.

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el o los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. (Superintendencia de Bancos del Ecuador, 2012)

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;

4.3.8.10 Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

4.3.8.12 Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas;

4.3.8.13 Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas. (Superintendencia de Bancos del Ecuador, 2012)

2.4 Marco Referencial

Lo que sucede en el Ecuador es que no existe Instituciones que certifiquen, de hecho en el país vecino Colombia si tienen entidades encargadas de certificar PCI-DSS por ejemplo *IQ Information Quality* es una empresa colombiana especializada en proveer servicios de seguridad en pagos electrónicos, teniendo como base estándares y mejores prácticas de la industria tales como: ITIL, ISO 27001, CobiT, PCI-DSS. Es la primera compañía certificada como QSA en Colombia por el PCI SSC para realizar las evaluaciones de cumplimiento de PCI-DSS a los comercios, bancos y proveedores de servicio en Latino América y el Caribe, permitiendo así que países de Latino América puedan tener su certificación. (Infomation Quality, 2013)

Si se parte del hecho de que cada uno de los bancos hace la calificación de riesgo y define el producto que va a entregar al cliente, una vez que ese plástico es entregado comienza a la actividad de servicio. Gráficamente la empresa está en todo lo que es la cadena de procesamiento, lo que tiene que ver con el back office active.

Credimatic como ejemplo de PCI-DSS es el primer procesador certificado del Estándar en el Ecuador. En diciembre de 2010 inició un proceso de renovación de plataforma tecnológica, la cual debía estar en consonancia con la estrategia que se había definido

para la entidad. Es por eso que hizo una invitación a nivel mundial, para que diferentes miembros presentaran propuestas en torno a esta plataforma tecnológica.

Por otra parte el banco de Guayaquil recibió la certificación PCI-DSS, luego de cumplir con todas las normas de seguridad de datos de la industria de tarjetas de pago. El cual inició el proceso de certificación en 2009, finalmente en diciembre de 2011 alcanzó la certificación, siendo el primer banco del Ecuador en obtenerla para todos sus procesos como emisor, operador y adquirente. (BANCO DE GUAYAQUIL, 2012)

Es importante mencionar que Pacificard es un servicio de banco del Pacifico, que en el año 2011 completo exitosamente la certificación del Estándar PCI-DSS; en el 2012 PCI le otorgó nuevamente la certificación de cumplimiento del Estándar de Seguridad de Datos de la Industria de Tarjeta de Pago versión 2.0. En el 2013 Pacificard inició con la auditoría en sitio del PCI-DSS, para mantener los niveles de seguridad de la información en todos los procesos y así brindar un servicio de calidad de datos para los clientes.

La normativa internacional PCI-DSS busca la protección total de los datos del tarjetahabiente en todos los procesos que ejecuta la institución, bloquea el acceso a información restringida, constituye uno de los principales mecanismos para evitar que los clientes sean víctimas de fraudes. (COUNCIL, PCI SECURITY, 2014)

“De esta manera, los banco certificados reafirman su compromiso con sus clientes al ofrecerles un servicio de calidad incrementando su seguridad al momento de realizar todas sus transacciones”. (BANCO DE GUAYAQUIL, 2012)

2.5 Formulación de Hipótesis

El análisis de la implementación del estándar PCI- DSS (Payment Card Industry – Data Security Standard) influye de manera significativa en la seguridad de la información en las transacciones con tarjetas de pago, ya que es una gran defensa contra los fraudes, permitiendo a las instituciones financieras garantizar la protección de los datos sensibles que manejan de sus clientes.

CAPITULO III

3. Marco Metodológico

3.1 Tipo de investigación

Los estudios descriptivos sirven para analizar como es y cómo se manifiesta un fenómeno y sus componentes (Metodología de la investigación, Daniel Behar 2008).

El tipo de investigación que se aplicó fue **"Investigación descriptiva",** dado que le permitirá al banco identificar claramente los requisitos necesarios para la implementación del estándar y que a su vez conozca los motivos por los cuales la información que poseen sobre sus clientes es de suma importancia y debe ser protegida.

El investigador solo se limita a la observación de los hechos tal como ocurren para luego describirlos, no buscará explicar mucho menos analizar las causas de esos hechos sino mostrarlos. De esta manera la investigación descriptiva brindará las bases cognoscitivas para los estudios descriptivos pues se generan hipótesis susceptibles de comprobación.

Según Tamayo (2004) Dice que: La investigación descriptiva trabaja sobre realidades de hechos y su característica fundamental es la de presentar una interpretación correcta.

La investigación es explicativa porque "Pretende establecer las causas de las funciones, que se estudian"; Hernández, (2003)… permitió determinar como es y cómo está la realidad de las variables y porque se trata de demostrar la relación causal entre las mismas.

3.2 Método

3.2.1 Método Inductivo:

"El método inductivo intenta ordenar la observación tratando de extraer conclusiones de carácter universal desde la acumulación de datos particulares" (Francis Bacon 1620).

El método que se aplicará en este caso es el inductivo, ya que se toma como punto de partida la información obtenida en la investigación realizada, en base a esto se obtendrá conclusiones generales enlazadas a la hipótesis que cual se brindará como solución al problema planteado.

En el cual se aplicó los pasos a seguir en este método que son la observación, experimentación, comprobación, abstracción y la generalización; para ir configurando la información necesaria con el propósito de alcanzar los objetivos de la investigación.

3.2.2 Método Sintético:

"Este método es un proceso de razonamiento que tiende a reconstruir un todo, a partir de los elementos distinguidos por el análisis; se trata en consecuencia de hacer una explosión metódica y breve, en resumen" (Euler Ruiz 2006).

El cual permite reunir y relacionar la información para así establecer conclusiones las cuales partieron de casos particulares a generalizaciones sobre el objeto de investigación planteado.

El investigador debe sintetizar las ventajas en la imaginación para luego establecer una explicación experimento.

3.2.3 Hipotético - Deductivo:

"Es el camino lógico para buscar la solución a los problemas planteados" (José Cegarra Sánchez 2004).

De las deducciones establecidas inicialmente se planteó una hipótesis, con la información proporcionada por los encuestados, luego del proceso de tabulación de las encuestas se realizó la comprobación de las mismas.

3.3 Población y Muestra

Dentro de la región costa del Ecuador, en la ciudad de Guayaquil, se han elegido a 20 bancos del sector privado como muestra a tomar de dicha población. Para calcular el tamaño de la muestra se utiliza la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2} \quad n = \frac{20 \text{ x } 0.5^2 \text{ x } 2.58^2}{(20-1)0.09^2 + 0.5^2 \text{ x } 2.58^2} = 18.30$$

Dónde:

n = El tamaño de la muestra.

N = Tamaño de la población.

σ = Desviación estándar de la población, valor constante de 0,5.

Z = Es un valor constante que, si no se tiene su valor, se lo toma en relación al 99% de confianza equivale a 2,58.

e = Límite aceptable de error muestral que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09).

Por lo tanto el tamaño de la Muestra será 18 entidades bancarias.

Técnicas e instrumentos de recolección de información

- ✓ **Revisión y análisis documental:** permite interpretar y clasificar la información existente referente al tema de estudio.
- ✓ **Encuestas:** permite recolectar datos a través de un cuestionario elaborado.

Debido a los estrictos niveles internos de seguridad de las instituciones bancarias se disminuyeron los niveles de profundidad de las preguntas estructuradas en la encuesta.

3.4 Encuesta del estándar PCI – DSS

La encuesta encierra las siguientes preguntas:

Marque con una X la respuesta que mejor se adapte al conocimiento que usted tiene acerca del estándar.

Pregunta General:

¿Conoce usted el estándar PCI-DSS?

SI ☐ NO ☐

Si la respuesta es afirmativa llenar la sección I de la encuesta, si repuesta es negativa llenar la sección II.

SECCIÓN I

Elegir la opción u opciones correctas.

1. ¿En qué clase de empresas opina Ud. que se puede aplicar el estándar PCI-DSS? (Opción única).

a) Institución Bancaria.
b) Institución Educativa.
c) Industria de Tarjetas de Débito.
d) Industria de Tarjetas de Pago.
e) Ninguna de las anteriores.

2. ¿Qué tipo de información trata de proteger el estándar PCI-DSS? (Opción única).

a) Información confidencial de los procesos de la organización.
b) Información confidencial del software implementado en la organización.
c) Datos confidenciales de los empleados de la organización.
d) Datos confidenciales del titular de la tarjeta.
e) Todas de las anteriores.

3. ¿Qué cambios cree usted que son indispensables realizar en la organización para aplicar el estándar? (Opción múltiple).

a) Adquisición de Equipos.
b) Mejoras de Software.
c) Encriptación de archivos.
d) Reforzar las políticas de seguridad de la empresa.
e) Todas las anteriores.

4. ¿Cómo cree usted que la aplicación del estándar beneficia a la seguridad de la información? (Opción única).

a) Protección de datos confidenciales del cliente durante la transacción.
b) Establece restricciones en el manejo de información.
c) Disminuye los riesgos de fraude en las transacciones de banca en línea.
d) Ayuda a incrementar el número de clientes en la organización.
e) Todas las anteriores.

5. ¿Cuánto es el tiempo estimado que le toma a la organización el proceso de implementación del estándar PCI-DSS? (Opción única).

a) 0 a 6 meses.
b) 6 a 12 meses.
c) 1 a 2 años.
d) 2 a 3 años.
e) 3 a 4 años.

6. ¿Conoce usted el rol de un QSA dentro de este proceso de aplicación del estándar PCI-DSS? (Opción única).

a) El QSA es una persona calificada por la empresa para validar el cumplimiento de las Normas PCI-DSS.
b) El QSA es una persona calificada por PCI SSC para validar el cumplimiento de las Normas PCI-DSS.
c) El QSA es un software ayuda a proteger datos confidenciales del dueño de la tarjeta.
d) El QSA es un estándar complementario de PCI-DSS.
e) Otro _____

7. ¿Qué versión del estándar cree Ud. que se implementará o se implementó en su organización?

a) 1.2
b) 2.0
c) 2.1
d) 3.0
e) Ninguna de las anteriores.

8. ¿Conoce usted las diferencias de la versión 2.0 con la versión 3.0 liberada en noviembre del 2013? En caso afirmativo, por favor explique.

9. ¿Recomendaría usted la implementación del estándar PCI-DSS a las demás instituciones financieras?

SI ☐ NO ☐

¿Por qué?

10. En la versión 3.0 se hizo un cambio referente a los requisitos del estándar. ¿Conoce Ud. cuál es el cambio que se efectuó?

a) Se disminuyó la cantidad de requisitos, haciendo que el proceso de implementación de la norma sea menos complejo.
b) Se agregó nuevos requisitos, con la finalidad de que reforzar la exigencia del estándar y garantizar la efectividad del mismo.
c) Aclara el objetivo o la intención del requisito, se asegura de que la redacción concisa de la norma exprese el objetivo deseado de los requisitos.
d) No conozco.

SECCIÓN II

1. Con el estándar PCI-DSS usted puede incrementar la seguridad de los datos de los Tarjetahabientes (titular de la tarjeta), aumentar la credibilidad en su institución, disminuir los fraudes en transacciones que impliquen el uso de las tarjetas de pago de débito y crédito, disminuye los riesgos de pérdidas financieras. ¿Dentro de estos cuál cree usted que es el punto más relevante? (Opción única).

a) Incrementar la seguridad de los datos.
b) Aumentar la credibilidad en su institución.
c) Disminuir los fraudes relacionados con las tarjetas de pago.

2. Ahora que conoce mejor el estándar. ¿Cómo cree usted que se beneficiaría la institución al implementar un estándar de este tipo? (Opción única)

a) Protección de datos confidenciales del cliente durante la transacción.
b) Establece restricciones en el manejo de información.
c) Disminuye los riesgos de fraude en las transacciones de banca en línea.
d) Ayuda a incrementar el número de clientes en la organización.
e) Todas las anteriores.

3. Con la seguridad en el manejo de datos del cliente que implica el uso del estándar, ¿Qué personal cree usted que es idóneo para el manejo de esta información? (Opción única).

a) Solo el personal dedicado al procesamiento de las transacciones.
b) Solo el personal dedicado al mantenimiento del software.
c) Solo el personal de alta Gerencia en Seguridad de Redes.
d) Solo el personal de Soporte Técnico.
e) Otro_____

4. ¿Cuáles creería Ud. que son las exigencias del estándar PCI-DSS al respecto del manejo de los datos de tarjetahabiente (titular de la tarjeta)? (Opción única).

a) Exige máxima confiabilidad y seguridad.
b) Exige mayor rapidez.
c) Exige adecuado procesamiento de los datos.
d) Ninguna de las anteriores.

5. ¿Cómo cree usted que se podría incrementar la seguridad de su institución al aplicar el estándar? (Opción única).

a) Implementando controles de acceso robustos.
b) Monitoreando las actividades que realizan los empleados
c) Monitoreando el acceso a la red regularmente.
d) Todas las anteriores.

6. ¿Realizan dentro de su institución campañas sobre seguridad de información?

SI ☐ NO ☐

7. ¿Conoce usted otros estándares de seguridad de información, dedicados exclusivamente a la industria de tarjetas de pago? En caso de respuesta afirmativa detallar.

SI ☐ NO ☐

8. ¿Cree Ud. que las políticas de seguridad dentro de su institución mejorarían con la aplicación del estándar PCI-DSS?

SI ☐ NO ☐

EN el caso de respuesta afirmativa, indique en que porcentaje cambiarían las políticas de seguridad con la aplicación del estándar. (Rango: 0 a 100%) _____

9. ¿Piensa usted que aplicar PCI-DSS es una buena práctica para mejorar la seguridad de la información en las instituciones financieras?

SI ☐ NO ☐

10. Luego de todos los puntos mencionados respecto al estándar ¿cree usted que se inclinaría a aplicar el estándar dentro de su institución?

SI ☐ NO ☐

3.4 Operacionalización de variables e indicadores

Declaración de Variables

Tabla 2. Declaración de las Variables

Variable Independiente	Variable Dependiente
Seguridad de los datos del Tarjetahabiente.	Conocimiento del Estándar PCI-DSS.

Elaborado por: Autores.

Tabla 3. Operacionalización de las Variables.

VARIABLE INDEPENDIENTE	DEFINICIÓN	INDICADORES	TÉCNICA
Seguridad de los datos del Tarjetahabiente	Percepción del estado de confianza o protección de los Datos en las transacciones con tarjetas de Pago.	✓ Políticas de Seguridad ✓ Disponibilidad del acceso a los datos. ✓ Aportes de las Entidades Bancarias	✓ Observación ✓ Investigación de campo ✓ Encuesta
VARIABLE DEPENDIENTE	**DEFINICIÓN**	**INDICADORES**	**TÉCNICA**
Conocimiento del Estándar PCI-DSS	Mayor o menor posibilidad de aceptación del Estándar de Seguridad.	✓ Efectividad de la Seguridad de los Datos al utilizar el Estándar PCI-DSS ✓ Estrategias de Seguridad de los datos. ✓ Factibilidad de establecer el Estándar PCI-DSS	✓ Observación ✓ Investigación de campo ✓ Encuesta

Elaborado por: Autores

Para HERRERA (2002), “la construcción de la información se opera en dos fases: plan para la recolección de información y plan para el procesamiento de información”.

3.5 Plan de recolección de información

Para Falcón y Herrera (2005) “se entiende como técnica, el procedimiento o forma particular de obtener datos o información”.

La Técnica utilizada en la investigación fue la encuesta y el instrumento un cuestionario estructurado con preguntas abiertas y cerradas, que se utilizará para el levantamiento de información relacionada con las variables en estudio y la situación actual, la misma que se aplicó al personal del Departamento de Tecnología y comunicación de las Entidades Financieras.

Para conseguir validez, se realizó los siguientes procedimientos:

- Elaboración de las matrices de Operacionalización de variables para estructurar el cuestionario

Para conseguir confiabilidad:

- Se aplicó normas científicas y técnicas para el tratamiento de los datos.

El plan para la recolección de información contempla estrategias metodológicas requeridas por los objetivos e hipótesis planteadas, se aplicó lo siguiente:

Elaboración, validación y reproducción de los instrumentos de recolección de la información.

Aplicación de los instrumentos en base al proceso:

a) Distribución de encuestas.
b) Explicación, ya que es una encuesta dirigida.

c) Satisfacción de inquietudes al momento de llenar el cuestionario, para que las respuestas sean contestadas en forma adecuada.
d) Revisión del Cuestionario, para evitar omisiones y errores.
e) Recolección de los cuestionarios de la encuesta aplicada.

3.6 Plan de procesamiento de la información

Se realizará el procesamiento de la información con el propósito de poder analizarla e interpretarla, con el fin de obtener de ellas las conclusiones necesarias para presentar la propuesta de la tesis.

a) Tabulación y elaboración de cuadros con los resultados obtenidos.
b) Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.
c) Comprobación de hipótesis.

Para procesar la información se utilizará el sistema operativo Windows 8.1, del paquete de office 2013, los programas microsoft word para la parte documental y microsoft excel, que facilita el análisis, interpretación y presentación de la información obtenida mediante la tabulación y gráficos.

CAPITULO IV

ANÁLISIS Y RESULTADOS

4.1 Análisis de la Situación Actual

En la actualidad lo que más ha causado malestar en las Instituciones Financieras es el robo de identidad, fraudes y violaciones de seguridad informáticos, estos son los tipos de problemas a los cuales se deben enfrentar las instituciones encargadas de transmitir, procesar y almacenar la información de las tarjetas de pago.

En el Ecuador, PCI está empezando a ser una realidad en la mayoría de las Instituciones Financieras que tramitan con tarjetas de Pago, algunas instituciones se encuentran gestionando el proceso de certificación, sin embargo sólo el 15% de las instituciones ya se encuentran certificas.

Cabe recalcar que debido a que la información que manejan las Instituciones Financieras es rigurosamente confidencial, por ese motivo la encuesta hace referencia al grado de conocimiento del Estándar PCI-DSS. El personal de dieciocho Instituciones Financieras encuestadas colaboró concediéndo la información solicitada en la encuesta. Para la protección de la identidad de estas instituciones, a las mismas se las nombra como A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q y R en el desarrollo de los resultados obtenidos.

4.2 Resultado de la Encuesta dirigida al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

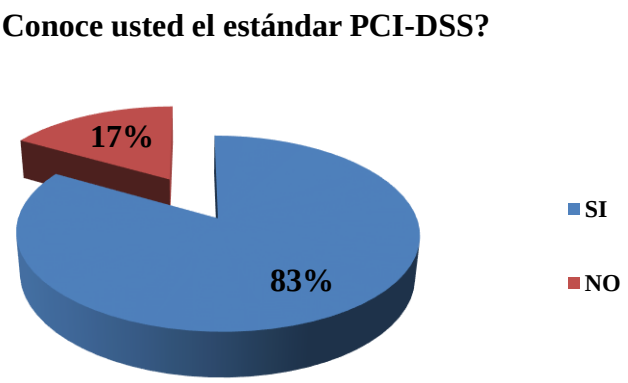
- **¿Conoce usted el estándar PCI-DSS?**

Tabla 4. Conocimiento del Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
SI	15	83%
NO	3	17%
Total	**18**	**100%**

Elaborado por: Autores
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 9. Conocimiento del Estándar PCI-DSS.



Elaborado por: Autores
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se puede apreciar que de los encuestados es decir el 83% conocen el estándar de Seguridad de información PCI-DSS, debido a que su Institución se encuentra certificada o en proceso de certificación Estándar PCI-DSS, mientras que otros indicaron que se encuentran en el proceso de certificación, por ello, están siendo capacitados con el tema de Seguridad, a diferencia, el 17% opinan que no tienen referencias claras acerca del estándar por ende su respuesta fue desconocen el estándar ya que sus instituciones cuentan con otro Estándar de Seguridad.

SECCIÓN I

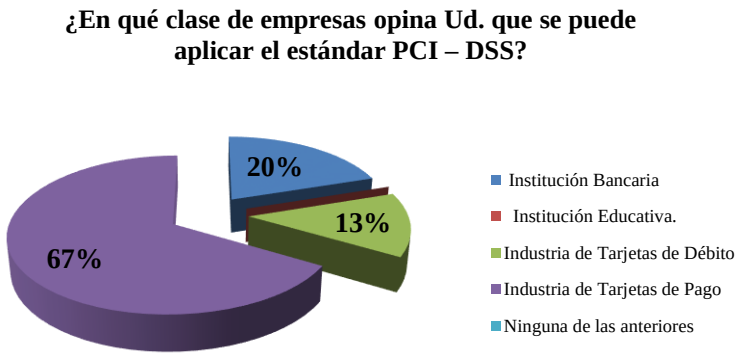
1. ¿En qué clase de empresas opina Usted que se puede aplicar el estándar PCI – DSS? (Opción única).

Tabla 5. Empresas que pueden aplicar el Estándar.

OPCIONES	RESULTADOS	PORCENTAJES
Institución Bancaria	3	20%
Institución Educativa.	0	0%
Industria de Tarjetas de Débito.	2	13%
Industria de Tarjetas de Pago.	10	67%
Ninguna de las anteriores.	0	0%
Total	**15**	**100%**

Elaborado por: Autores
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 10. Empresas que pueden aplicar el Estándar.



Elaborado por: Autores
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: El 67% tiene conocimientos de las Instituciones a las cuales se le aplica el Estándar de Seguridad PCI-DSS, el 20% opinan que solo se aplica a Instituciones Bancarias. Mientras que el 13% opina que solo se le aplica a la Industria de tarjetas de Débito, De las respuestas obtenidas se pudo observar que un porcentaje reducido no tiene conocimientos claros del Tipo de Empresa a la cual se debe aplicar el Estándar, más del 60% recalca que cualquier entidad que transmita, procese o almacene datos de tarjetas de crédito o débito debe cumplir el estándar en mención (Industria de Tarjetas de Pago).

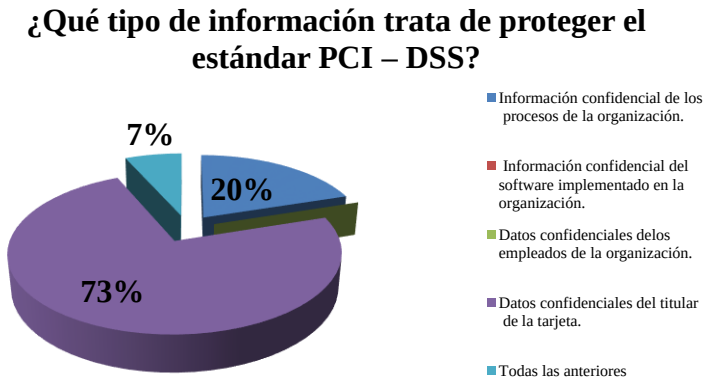
2. ¿Qué tipo de información trata de proteger el Estándar PCI – DSS? (Opción única).

Tabla 6. Información que trata de proteger el Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
Información confidencial de los procesos de la organización.	3	20%
Información confidencial del software implementado.	0	0%
Datos confidenciales de los empleados de la organización.	0	0%
Datos confidenciales del titular de la tarjeta.	11	73%
Todas las anteriores	1	7%
Total	**15**	100%

Elaborado por: Autores
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 11. Información que trata de proteger el Estándar PCI-DSS.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: El 73% de los encuestados está de acuerdo que el Estándar PCI-DSS protege datos confidenciales del Titular de la Tarjeta lo cual es esencial, el 20% opinan que sólo protege información confidencial de los procesos de la organización, mientras que el 7% indicó que protege la información confidencial de los empleados, los procesos de la organización, datos confidenciales del tarjetahabiente y datos confidenciales de los empleados. De las respuestas obtenidas se puede observar que el porcentaje más alto indica que el estándar protege los datos de los tarjetahabiente como el número de tarjeta, el nombre del titular y la fecha de expiración, así como también la información sensible que utilizan para las transacciones no presenciales.

3. ¿Qué cambios cree usted que son indispensables realizar en la organización para aplicar el estándar? (Opción múltiple).

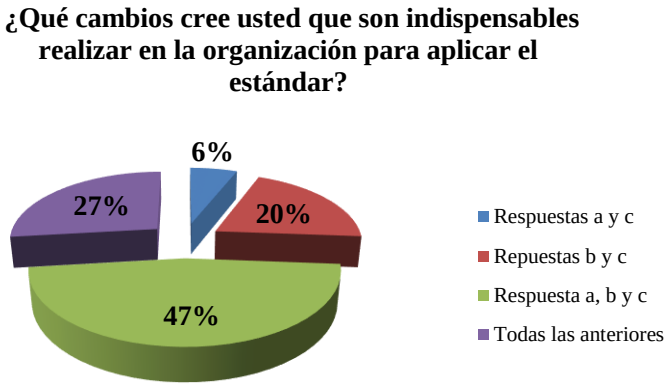
a) Adquisición de Equipos. b) Mejoras de Software. c) Encriptación de archivos. d) Reforzar las políticas de seguridad de la empresa. e) Todas las anteriores.

Tabla 7. Conocimiento de cambios indispensables para la aplicación del Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
Respuestas a y c	1	6%
Repuestas b y c	3	20%
Respuesta a, b y c	7	47%
Todas las anteriores	4	27%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 12. Conocimiento de cambios indispensables para la aplicación del Estándar PCI-DSS.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: El 47% de los encuestados está de acuerdo que se debe reforzar las políticas de seguridad de su institución, adquirir equipos y mejorar el software, el 27% opinan que todas las opciones propuestas son necesarias para la implementación del Estándar, el 20% indica que se debe mejorar el Software y enviar la información encriptada, mientras que el 6% opina que se debería adquirir equipos nuevos avanzados y respecto a la información sea enviada de forma encriptada. De las respuestas obtenidas se puede llegar a la conclusión que más del 50% de los encuestados tiene conocimiento referente a los cambios indispensables que necesita su organización para poder Certificarse con PCI-DSS.

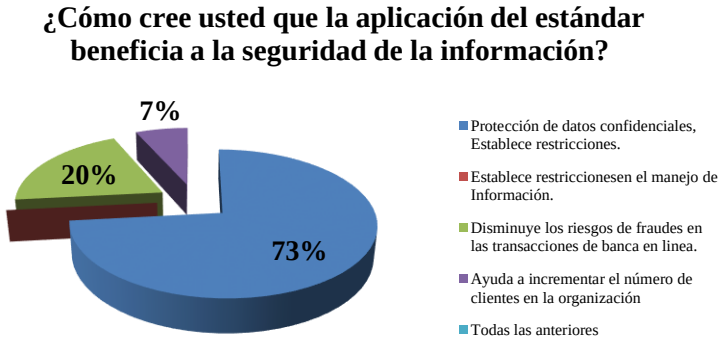
4. ¿Cómo cree usted que la aplicación del estándar beneficia a la seguridad de la información? (Opción única).

Tabla 8. Beneficia la aplicación del Estándar a la Seguridad.

OPCIONES	RESULTADOS	PORCENTAJES
Protección de datos confidenciales, Establece restricciones.	11	73%
Establece restricciones en el manejo de Información.	0	0%
Disminuye los riesgos de fraudes en las transacciones de banca en línea.	3	20%
Ayuda a incrementar el número de clientes en la organización	1	7%
Todas las anteriores	0	0%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 13. Beneficia la aplicación del Estándar a la Seguridad.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se puede apreciar que la mayor parte de los encuestados es decir el 73% está de acuerdo que el Estándar beneficiaria la Protección de datos confidenciales del cliente durante la transacción, lo cual favorece en cuanto a la confianza que tendrían los clientes de Tarjetas de Pago, el 20% opinan que se disminuye los riesgos de fraude en las transacciones de banca en línea, mientras que el 7% cree el beneficio seria el incremento de clientes en la organización. De las respuestas obtenidas se llega a la

conclusión, que la mayoría de los encuestados indican que es muy beneficioso para la organización contar con el Estándar de Seguridad PCI-DSS.

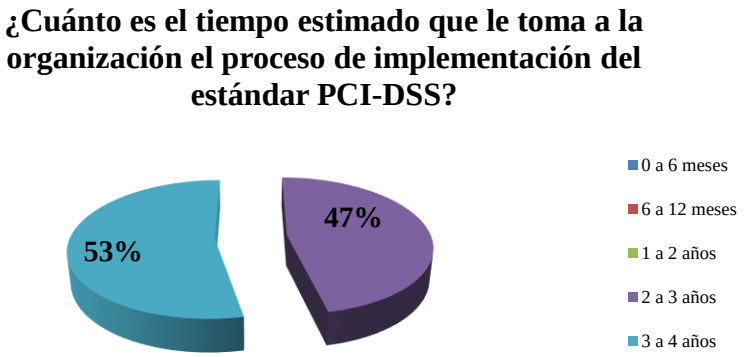
5. ¿Cuánto es el tiempo estimado que le toma a la organización el proceso de implementación del Estándar PCI-DSS? (Opción única).

Tabla 9. Tiempo del Proceso de Implementación del Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
0 a 6 meses	0	0%
6 a 12 meses	0	0%
1 a 2 años	0	0%
2 a 3 años	7	47%
3 a 4 años	8	53%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 14. Tiempo del Proceso de Implementación del Estándar PCI-DSS.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: El 53% está de acuerdo que el proceso de implementación del Estándar tardaría de 3 a 4 años, lo cual es de gran beneficio ya que para poder certificarse la organización debe cumplir los 12 requisitos establecidos, mientras que el 47% opinan que el proceso de certificación debería durar de 2 a 3 años. De las respuestas obtenidas se llega a la conclusión que más del 50% de los encuestados indicarón que lleva varios años el proceso de certificación del Estándar PCI-DSS, ya que para certificarse se necesita cumplir varios requisitos.

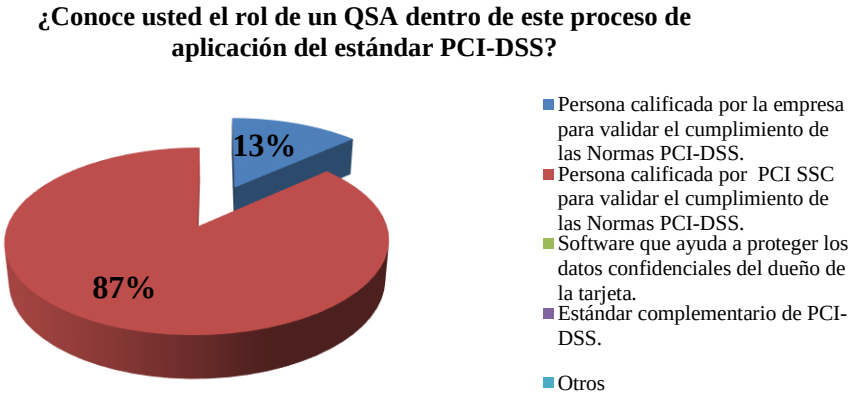
6. ¿Conoce usted el rol de un QSA dentro de este proceso de aplicación del estándar PCI-DSS? (Opción única).

Tabla 10. Conocimiento sobre el Rol de un QSA.

OPCIONES	RESULTADOS	PORCENTAJES
Persona calificada por la empresa para validar el cumplimiento de las Normas PCI-DSS.	2	13%
Persona calificada por PCI SSC para validar el cumplimiento de las Normas PCI-DSS.	13	87%
Software que ayuda a proteger los datos confidenciales del dueño de la tarjeta.	0	0%
Estándar complementario de PCI-DSS.	0	0%
Otros	0	0%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 15. Conocimiento sobre el Rol de un QSA.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que el 87% de las personas encuestadas coinciden que el Rol del QSA es auditar por ende es una persona calificada por PCI SSC para validar el cumplimiento de las Normas PCI-DSS, mientras que el 13% indica que es una persona interna a la institución financiera encargada de validar el cumplimiento de PCI-DSS. De las respuestas obtenidas se llega a la conclusión que el personal tienen claro cuál es la función del QSA, es un Auditor que está autorizado a realizar auditorías on-site

del estándar PCI-DSS que permitan certificar el cumplimiento de las marcas o las Entidades Bancarias.

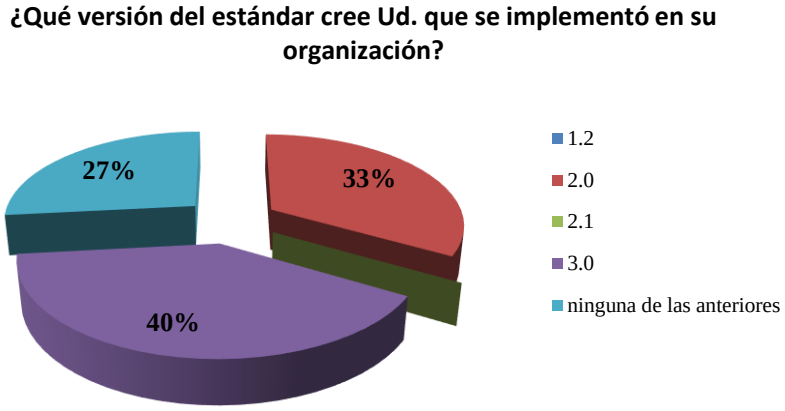
7. ¿Qué versión del estándar cree Ud. que se implementará o se implementó en su organización? (Opción única).

Tabla 11. Versión de Estándar en su organización.

OPCIONES	RESULTADOS	PORCENTAJES
1.2	0	0%
2.0	5	33%
2.1	0	0%
3.0	6	40%
Ninguna de las anteriores	4	27%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 16. Versión de Estándar en su organización.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 40% indico que el estándar implementado en su organización era la Versión 2.0 de PCI-DSS, pero que migrarían a la nueva versión actual, el 60% se encuentran en proceso de Certificación e indicaron que se implementará una versión actual mientras que otros no tenían idea de la versión que se implementará.

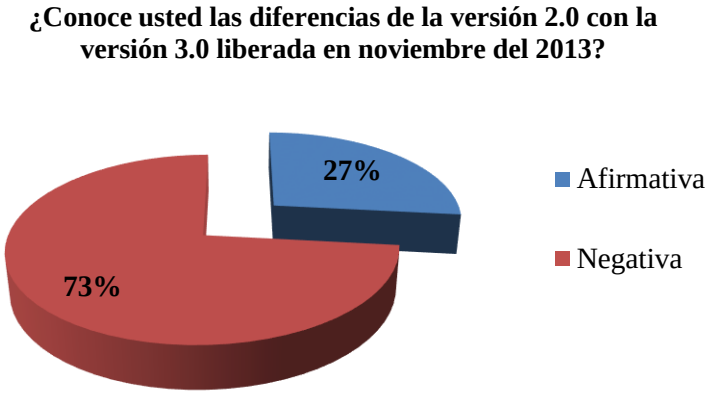
8. ¿Conoce usted las diferencias de la versión 2.0 con la versión 3.0 liberada en noviembre del 2013? En caso afirmativo, por favor explique.

Tabla 12. Conocimiento de las diferencias entre las Versiones 2.0 y 3.0.

OPCIONES	RESULTADOS	PORCENTAJES
Afirmativa	4	27%
Negativa	11	73%
Total	**15**	100%

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 17. Conocimiento de las diferencias entre las Versiones 2.0 y 3.0.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 73% desconoce las diferencias que existen entre ambas versiones, pero indicaron que tienen claro que es una versión mejorada del Estándar PCI-DSS, mientras que el 27% indica que conocen muy poco de las diferencias pero mencionaron algunas que en la Versión 3.0 se han agregado requisitos técnicos. De las respuestas obtenidas se llega a la conclusión que es necesario que el personal tenga conocimiento que en la nueva versión se aclaran los requisitos existentes y añaden requisitos técnicos adicionales.

9. ¿Recomendaría usted la implementación del estándar PCI-DSS a las demás instituciones financieras?

Tabla 13. Recomendaría la implementación del Estándar.

OPCIONES	RESULTADOS	PORCENTAJES
SI	15	100%
NO	0	0%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 18. Recomendaría la implementación del Estándar.

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se puede observar que de la población bancaria encuestada, El 100% está totalmente de acuerdo en el que las Instituciones Financieras cumplan con el Estándar de Seguridad PCI- DSS ya que le trae muchos Beneficios como por ejemplo que el tarjetahabiente confié sus datos a dicha institución. De las respuestas obtenidas se llega a la conclusión que las personas encuestadas recomendarían la implementación de dicho Estándar porque consideran que el mismo puede ayudarles a fomentar la confianza de sus clientes, garantizando la protección de datos.

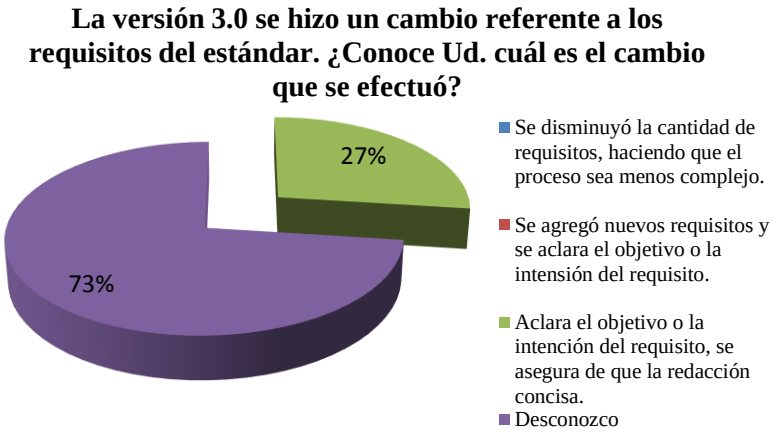
10. En la versión 3.0 se hizo un cambio referente a los requisitos del estándar. ¿Conoce Ud. cuál es el cambio que se efectuó? (Opción única).

Tabla 11. Conocimiento el cambio que se efectuó en la Versión 3.0.

OPCIONES	RESULTADOS	PORCENTAJES
Se disminuyó la cantidad de requisitos, haciendo que el proceso sea menos complejo.	0	0%
Se agregó nuevos requisitos y se aclara el objetivo o la intensión del requisito.	0	0%
Aclara el objetivo o la intención del requisito, se asegura de que la redacción concisa.	4	27%
Desconozco	11	73%
Total	**15**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 19. Conoce usted el cambio que se efectuó en la Versión 3.0.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 73% desconoce los cambios de la nueva versión del Estándar PCI-DSS, mientras que el 27% tiene claro que los cambios realizados en la nueva versión aclara los objetivo o la intensión de los requisitos, este cambio se asegura, la redacción concisa, para que la norma exprese el objetivo deseado de los requisitos.

SECCIÓN II

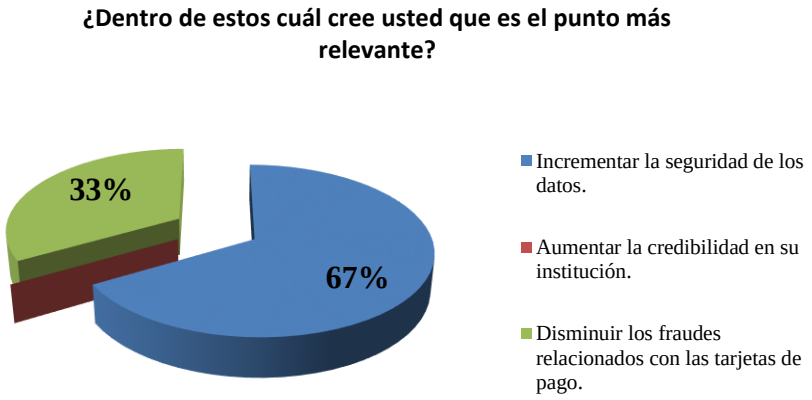
1. **Con el estándar PCI-DSS usted puede incrementar la seguridad de los datos de los Tarjetahabientes (titular de la tarjeta), aumentar la credibilidad en su institución, disminuir los fraudes en transacciones que impliquen el uso de las tarjetas de pago de débito y crédito, los riesgos de pérdidas financieras. ¿Dentro de estos cuál cree usted que es el punto más relevante? (Opción única).**

Tabla 14. Punto más relevante del Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
Incrementar la seguridad de los datos.	2	67%
Aumentar la credibilidad en su institución.	0	0%
Disminuir los fraudes relacionados con las tarjetas de pago.	1	33%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 20. Punto más relevante del Estándar PCI-DSS.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 67% está de acuerdo que el estándar PCI-DSS incrementa la seguridad de los datos de los Tarjetahabientes, mientras que el 33% opina que el estándar permite disminuir los fraudes en transacciones que impliquen el uso de las tarjetas de pago de débito y crédito. De las respuestas obtenidas se llega a la conclusión que más del 60% indica que el punto más relevante que tiene el Estándar PCI-DSS es incrementar la seguridad de los datos del

tarjetahabiente, ya que son datos muy sensible, una opción es cifrarlos antes de su proceso de transmisión en redes públicas, para así proteger los datos de hackers y otros criminales cibernéticos que pretendan robar la información.

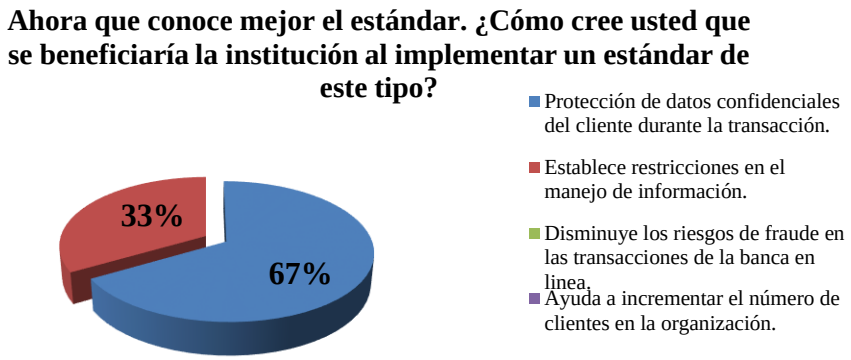
2. Ahora que conoce mejor el estándar. ¿Cómo cree usted que se beneficiaría la institución al implementar un estándar de este tipo?

Tabla 15. Beneficiaría con este Estándar a su Institución.

OPCIONES	RESULTADOS	PORCENTAJES
Protección de datos confidenciales del cliente durante la transacción.	2	67%
Establece restricciones en el manejo de información.	1	33%
Disminuye los riesgos de fraude en las transacciones de la banca en línea.	0	0%
Ayuda a incrementar el número de clientes en la organización.	0	0%
todas las anteriores	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 21. Beneficiaría con este Estándar a su Institución.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 67% está de acuerdo que el Estándar beneficia la Protección de los datos confidenciales del Cliente durante la transacción, mientras el 33% opinan que el estándar PCI-DSS beneficia mucho a las la instituciones financieras que lo implementen, ya que establece restricciones en

el manejo de la información. De las respuestas obtenidas se llega a la conclusión que dicho estándar beneficiaria totalmente a la Institución que lo implemente, ya que al crear una protección de datos estableciendo restricciones en el manejo de dicha información, se disminuye los riegos de fraudes electrónicos.

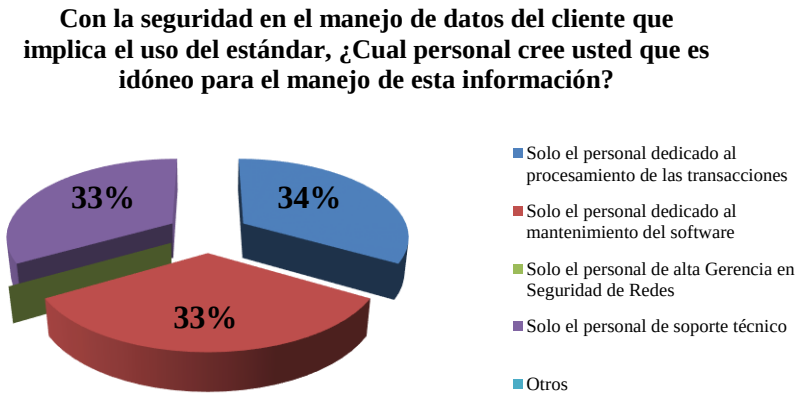
3. Con la seguridad en el manejo de datos del cliente que implica el uso del estándar, ¿Qué personal cree usted que es idóneo para el manejo de esta información?

Tabla 16. Personal idóneo para manejar la información confidencial del Cliente.

OPCIONES	RESULTADOS	PORCENTAJES
Solo el personal dedicado al procesamiento de las transacciones	1	33%
Solo el personal dedicado al mantenimiento del software	1	33%
Solo el personal de alta Gerencia en Seguridad de Redes	0	0%
Solo el personal de soporte técnico	1	33%
Otros	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 22. Personal idóneo para manejar la información confidencial del Cliente.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 33% está de acuerdo que el personal idóneo para manejar los datos confidenciales del Tarjetahabiente es el

personal dedicado al procesamiento de las transacciones, el 33% opinan que el personal dedicado al mantenimiento del software es el idóneo para manejar los datos confidenciales, mientras que el 33% manifestó que el personal idóneo es el personal de soporte técnico. De las respuestas obtenidas se llega a la conclusión que más del 50% de los encuestados no tienen claro cuál sería el personal idóneo para manejar los datos confidenciales del Tarjetahabiente.

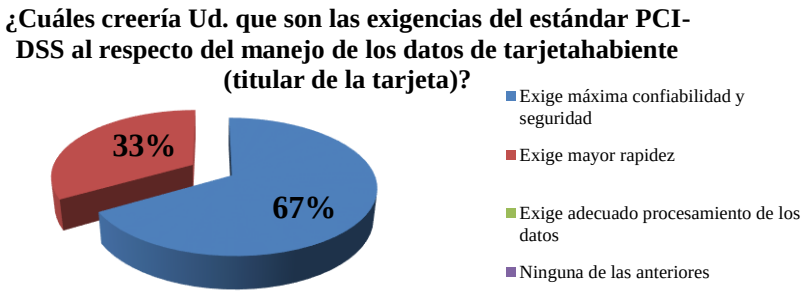
4. ¿Cuáles creería Ud. que son las exigencias del estándar PCI-DSS al respecto del manejo de los datos de tarjetahabiente (titular de la tarjeta)?

Tabla 17. Exigencias del Estándar PCI-DSS en el manejo de datos del tarjetahabiente.

OPCIONES	RESULTADOS	PORCENTAJES
Exige máxima confiabilidad y seguridad.	2	67%
Exige mayor rapidez.	1	33%
Exige adecuado procesamiento de los datos.	0	0%
Ninguna de las anteriores	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 23. Exigencias del Estándar PCI-DSS en el manejo de datos del tarjetahabiente.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 67% manifestó que el Estándar PCI-DSS exige máxima confiabilidad y seguridad de los datos confidenciales del Tarjetahabiente, mientras el 33% indico que el Estándar PCI-DSS exige mayor rapidez de datos confidenciales del tarjetahabiente. De las respuestas obtenidas se llega a la conclusión que más del 60% de los encuestados están de acuerdo

que el estándar exige una seguridad extrema, se recalca que una de la exigencias más importantes es el adecuado procesamiento de datos confidenciales del tarjetahabiente.

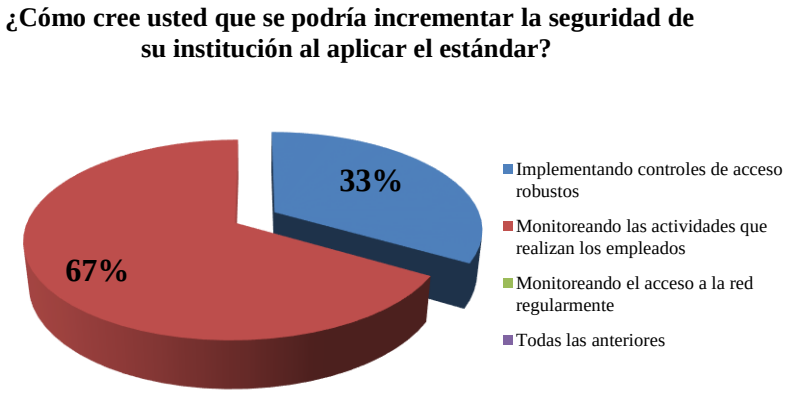
5. ¿Cómo cree usted que se podría incrementar la seguridad de su institución al aplicar el estándar?

Tabla 18. Conocimiento de cómo incrementa la seguridad de su institución aplicar el Estándar.

OPCIONES	RESULTADOS	PORCENTAJES
Implementando controles de acceso robustos	1	33%
Monitoreando las actividades que realizan los empleados	2	67%
Monitoreando el acceso a la red regularmente	0	0%
Todas las anteriores	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 24. Conocimiento de cómo incrementa la seguridad de su institución aplicar el Estándar.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria

Análisis: Se observa que de la población bancaria encuestada, el 67% manifestó que se podría incrementar la seguridad de su institución monitoreando las actividades que realizan los empleados, mientras el 33% indico que se podría incrementar la implementando controles de accesos robustos. De las respuestas obtenidas se llega a la conclusión que menos del 40% de los encuestados están de acuerdo que se podría

incrementar la seguridad de su institución con controles de acceso robusto, lo cual es factible, por ello también se debe recalcar, que se debería monitorear el acceso a la red regularmente ya que se procesan y se transmiten datos confidenciales del tarjetahabiente.

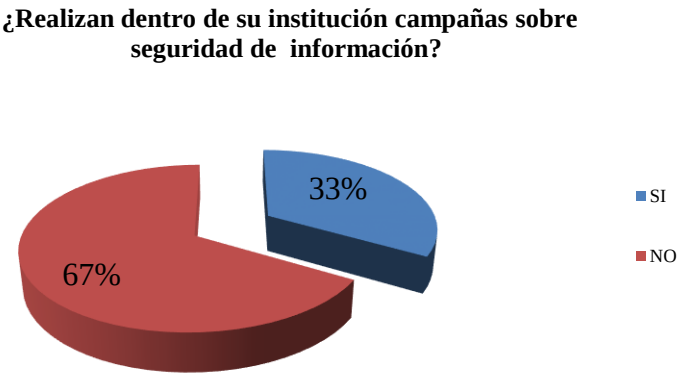
6. ¿Realizan dentro de su institución campañas sobre seguridad de información?

Tabla 19. Realizan campañas de Seguridad en su Institución.

OPCIONES	RESULTADOS	PORCENTAJES
SI	1	33%
NO	2	67%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 25. Realizan campañas de Seguridad en su Institución.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se observa que de la población bancaria encuestada, el 67% indico que en su institución no difunden campañas de Seguridad ya que creen que no es necesario, mientras que el 33% opinan que es gran ayuda para su conocimiento propio las campañas de Seguridad que difunden en su Institución, ya que mediante las misma se puede prevenir la fuga de información dentro de la Institución.

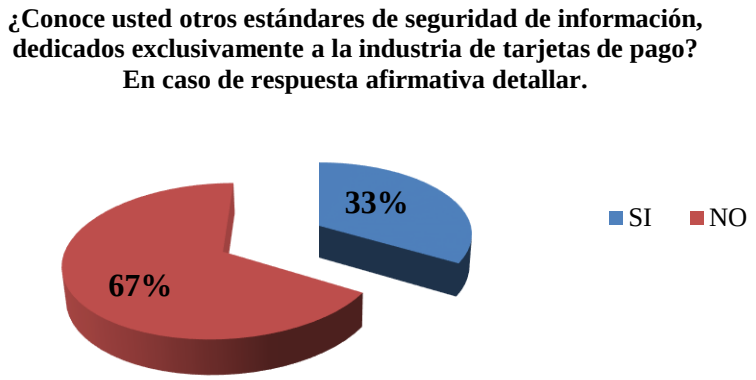
7. ¿Conoce usted otros estándares de seguridad de información, dedicados exclusivamente a la industria de tarjetas de pago? En caso de respuesta afirmativa detallar.

Tabla 20. Conocimiento de otros Estándares de Seguridad de Tarjetas de Pago.

OPCIONES	RESULTADOS	PORCENTAJES
SI	1	33%
NO	2	67%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 26. Conocimiento de otros Estándares de Seguridad de Tarjetas de Pago.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria

Análisis: Se observa que el 67% indico que desconoce la existencia de otro Estándar de Seguridad para proteger la información de las tarjetas de pago, mientras que el 33% opinan que existen otros estándares de seguridad como la ISO y Cobit pero indicaron que no están totalmente seguros si son o no para la seguridad de las tarjetas de pago. De las respuestas obtenidas se llega a la conclusión que más del 60% desconocen la existencia de otros Estándares de Seguridad, cabe indicar que el Estándar de Seguridad PCI-DSS es el más utilizado a nivel mundial para la protección de los datos de las tarjetas de pagos mientras que los demás estándares son un complemento de Seguridad para PCI-DSS, los cuales también tienen políticas de seguridad y son implementado también en las instituciones que manejan información confidencial.

8. ¿Cree Ud. que las políticas de seguridad dentro de su institución mejorarían con la aplicación del estándar PCI-DSS?

Tabla 21. Conocimiento de las políticas de seguridad mejorarían con la implementación del Estándar PCI-DSS.

OPCIONES	RESULTADOS	PORCENTAJES
SI	3	100%
NO	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 27. Conocimiento de las políticas de seguridad mejorarían con la implementación del Estándar PCI-DSS.

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se puede observar que el 100% opina que las políticas de seguridad de su institución mejorarían, y mencionaron que las políticas de seguridad son guías que permiten asegurar la protección y la integridad de los datos que manejan, e indicaron que la institución mejoraría en un 89% su seguridad.

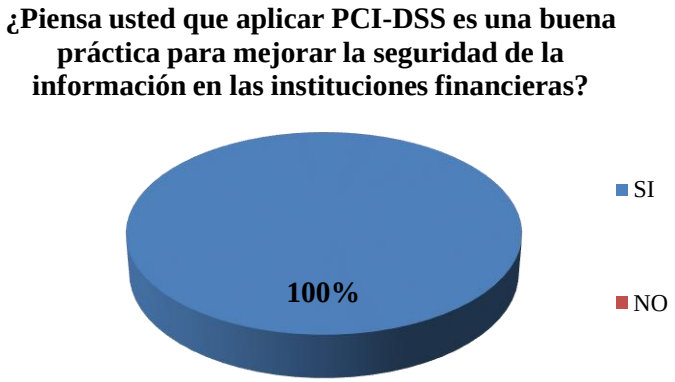
9. ¿Piensa usted que aplicar PCI-DSS es una buena práctica para mejorar la seguridad de la información en las instituciones financieras?

Tabla 22. Conocimiento al aplicar el Estándar mejorara la Seguridad de la Información en Instituciones Financieras.

OPCIONES	RESULTADOS	PORCENTAJES
SI	3	100%
NO	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 28. Conocimiento al aplicar el Estándar mejorara la Seguridad de la Información en Instituciones Financieras.



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Análisis: Se puede observar que de la población bancaria encuestada, el 100% opinan que al aplicar el Estándar PCI-DSS en las Instituciones Financieras mejorara la seguridad de la Información, cabe indicar que es una buena práctica de seguridad que se certifique con el Estándar PCI-DSS una institución que maneje transacciones con tarjetas de pago.

10. Luego de todos los puntos mencionados respecto al estándar ¿cree usted que se inclinaría a aplicar el estándar dentro de su institución?

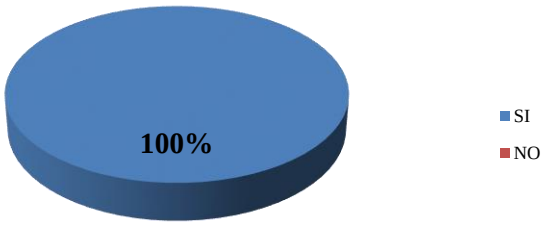
Tabla 23. Aplicaría el estándar dentro de su Institución.

OPCIONES	RESULTADOS	PORCENTAJES
SI	3	100%
NO	0	0%
Total	**3**	**100%**

Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

Figura 29. Aplicaría el estándar dentro de su Institución.

Luego de todos los puntos mencionados respecto al estándar ¿cree usted que se inclinaría a aplicar el estándar dentro de su institución?



Elaborado por: Autores.
Fuente: Encuesta Realizada al personal del Departamento de Tecnología y Comunicación de la Entidad Bancaria.

.

Análisis: Se observa que de la población bancaria encuestada, el 100% opina que el Estándar de Seguridad es opción primordial e indicarón que están seguros que al aplicar el Estándar PCI-DSS se mejoraría la seguridad dentro de su institución financiera con respecto a las transacciones de los datos del tarjetahabiente.

4.3 Verificación de Hipótesis.

La validación de la Hipótesis del trabajo: “Análisis de la implementación del estándar PCI-DSS en la seguridad de la información dentro de una institución financiera”, se ratifica como verdadera con los resultados de las encuestas realizadas a los empleados del departamento de sistemas y comunicaciones de las entidades bancarias, ya que mayoritariamente recomiendan que la aplicación del estándar PCI-DSS como mejora en el aspecto de seguridad de la información de su organización.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

- Las tarjetas de crédito y débito ligadas a un titular de tarjeta, conocidas comúnmente como dinero plástico se han convertido en el medio de pago y consumo de uso más frecuente, por tanto es indispensable aplicar los mecanismos de protección necesarios para salvaguardar la seguridad de los datos confidenciales que se encuentran inmersos en la misma.

- Con la aplicación de la encuesta al personal del departamento de Sistemas se llegó a la conclusión que más del 50% de los encuestados tienen conocimiento claros referente a las normativas de seguridad, e indicarón que las mismas permiten definir medidas de protección adecuadas para el tratamiento, procesamiento o almacenamiento de información, por tal razón consideran que todas las instituciones deben certificarse con cualquier estándar de seguridad internacional como lo estipula la ley de bancos y Seguros, si bien es cierto seria de mucha ayuda que todas instituciones tengan conocimiento del estándar PCI-DSS ya que es una solución efectiva para garantizar la seguridad de los datos confidenciales del tarjetahabiente.

- Con la encuesta realizada se pudo concluir que menos del 25% de las instituciones financieras no se encuentran certificadas con el Estándar de Seguridad PCI-DSS, debido a que sus proveedores de servicios son quienes se encuentran certificados con el estándar de seguridad PCI-DSS.

5.2 Recomendaciones.

La institución Bancaria debe abarcar totalmente los lineamentos de PCI-DSS, ya que usualmente se enfoca en los aspectos tecnológicos, dejando en un segundo plano los aspectos documentales o procedimentales, que son esenciales para asegurase de que el auditor QSA, certifique que la organización alcanzó el nivel de cumplimiento exigido por el estándar.

Con este análisis se identificó que el 67% delos bancos tomados como parte de la muestra no se imparten campañas de seguridad lo que es un punto clave para que el personal este altamente capacitado respecto al correcto uso y manejo de la información, por lo tanto se deben realizar programas de concientización de seguridad de información para todas las áreas involucradas dentro de la organización.

Se aconseja a las entidades bancarias impartir charlas, al personal encargado del procesamiento de datos de titular de tarjetas, sobre el tipo de información que deben o no almacenar ya que el 80% de la población bancaria encuestada no tiene claramente identificados los datos que deben protegerse para el cumplimiento de los lineamientos de PCI-DSS.

Incrementar las campañas informativas dirigidas a los clientes del banco, sobre las precauciones que deben emplearse al momento de realizar transacciones desde los diversos canales como: ATM, POS, banca electrónica y banca móvil.

CAPITULO VI

PROPUESTA

6.1 Datos Informativos

6.1.1 Titulo

"Diseño de una Guía de Auditoria de Sistemas que permita evaluar el control interno de una Institución Financiera basado en los Estándares PCI-DSS en la Seguridad de la Información"

6.1.2 Proponentes

- Andrea Jacqueline Mejía Villegas
- Zoila Alexandra Calle Parrales

6.1.3 Objeto de Estudio

Departamento de tecnología y comunicaciones del banco A, ubicado en la ciudad de Guayaquil, a quien se le ha asignado una letra, debido al acuerdo de confidencialidad establecido con la institución.

6.1.4 Beneficiarios

- Funcionarios del banco
- Clientes del banco (Titulares de Tarjetas)

6.2 Antecedentes de la propuesta

El departamento de tecnología y comunicaciones del banco A, es una dependencia que necesita realizar cambios debido al negocio de tarjetas de pago en el que está inmersa,

para el cual se enfrenta al reto de implementar mejoras respecto al uso y manejo de la información enmarcada dentro del contexto de procesamiento de los datos del titular de la tarjeta; es de suma importancia que este departamento cuente con un estudio que le facilitará la ejecución de las actividades previas al proceso de implementación del estándar PCI-DSS de forma clara.

El análisis implica un estudio descriptivo respecto al estándar, sus lineamientos y el estado en que el banco A se encuentra para iniciar el proceso de implementación del mismo, motivo por el cual se considera que este trabajo servirá para orientar a la institución sobre cuáles son las medidas que debe tomar, para alcanzar metas de seguridad establecidas y obtener resultados en beneficio de la empresa.

Previo al análisis se deben conocer las características del negocio, por este motivo se describe que banco A, ofrece una gama de productos y servicios a sus clientes como los que se detallan a continuación:

Productos:

Cuentas

- ✓ Ahorro
- ✓ Corriente

- **Créditos**

  - ✓ Hipotecarios
  - ✓ Comerciales
  - ✓ Personales

- **Tarjetas**

  - ✓ Débito

Servicios:

- Cobros
- Pagos
- Transferencias Bancarias
- Transferencias Interbancarias

El banco A ofrece el producto de tarjetas de débito, que contienen los datos confidenciales del tarjetahabiente, por tanto deben tener mecanismos de protección para el procesamiento de las mismas.

6.3 Justificación

Es importante señalar que el análisis de la implementación del estándar PCI-DSS, es la base que permitirá identificar los mecanismos de seguridad que se llevan actualmente en la institución, poniendo de manifiesto que no solo se requiere implementar medidas robustas de control y acceso, también se debe fomentar dentro de la organización la cultura de la información.

En este sentido el estudio se puede enfocar a todas las personas vinculadas al departamento de tecnología y comunicaciones, para validar un control interno, asegurar la información y consolidar el cumplimiento de la normativa.

Este estudio demostrará la importancia de contar con medidas de control de información como las que ofrece estándar PCI-DSS, ayudando al banco a tener una idea concreta respecto a la preparación que debe tener previo a la implementación del mismo, es fundamental la ejecución de un estudio, para determinar los puntos que el banco debe mejorar, para incrementar su nivel de seguridad y poder garantizar a sus clientes la integridad de sus datos.

Mediante la elaboración del análisis se dan a conocer las mejores prácticas de seguridad que debe adoptar el banco, para que las mismas contribuyan de manera favorable, al cumplimiento eficaz y eficiente de los lineamientos de PCI-DSS.

Aplicando el estándar en el banco, se pueden minimizar los fraudes relacionados con las tarjetas de crédito, lo que proporciona confiablidad de los datos del tarjetahabiente quienes requieren que el banco al que le confían su dinero, cumpla con las medidas de seguridad de tal forma que sus finanzas no se vean comprometidas.

6.4 Objetivos

6.4.1 Objetivo General

Dar a conocer los requisitos necesarios que deben cumplir los sistemas de control interno de las Empresas Financieras para garantizar la seguridad de la información en el procesamiento, almacenamiento y/o transmisión de datos de los tarjetahabientes.

6.4.2 Objetivos Específicos

- Establecer los procedimientos de seguridad de información para garantizar la integridad y fiabilidad de los procesos internos

- Dar a conocer las diferentes herramientas y técnicas de Auditoría asistida para mejorar el control interno de la información.

6.5 Análisis de factibilidad

El presente estudio hace referencia a un conjunto de procedimientos interrelacionados que pueden corresponder a un departamento o la totalidad de una dependencia.

Para la elaboración de este análisis, los procedimientos de seguridad deberán ser específicos, de tal forma que se presenten como eje central para llevar a cabo

diversas actividades para la obtención de un alto nivel de protección de la información de la institución.

La propuesta de tesis, toma como punto de partida los procedimientos internos de seguridad de la organización y el nivel de conocimiento del estándar que tienen los empleados del departamento de sistemas y comunicaciones, es factible de llevarse a la práctica ya que la institución colabora con la información requerida siempre y cuando se manejen sus datos de forma anónima.

6.6 Fundamentación

La aplicación del estándar PCI-DSS (Payment Card industry – Data security standar), sirve como ayuda al cumplimiento de las exigencias de la superintendencia de bancos respecto al correcto procesamiento de las transacciones asociadas a las tarjetas de pago y referentes al uso y manejo de canales electrónicos, que deben ser monitoreados constantemente.

Por tanto de esta manera se mantiene una interrelación e identificación de los lineamientos de la estructura orgánica vigente y autorizada por la Superintendencia de bancos y seguros del Ecuador.

En el libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero", la Junta Bancaria del Ecuador JB-2012-2148, define en el artículo N°1, la protección contra la clonación de tarjetas, y en el artículo N°2, Medidas de seguridad en canales electrónicos. (Superintendencia de Bancos del Ecuador, 2012).

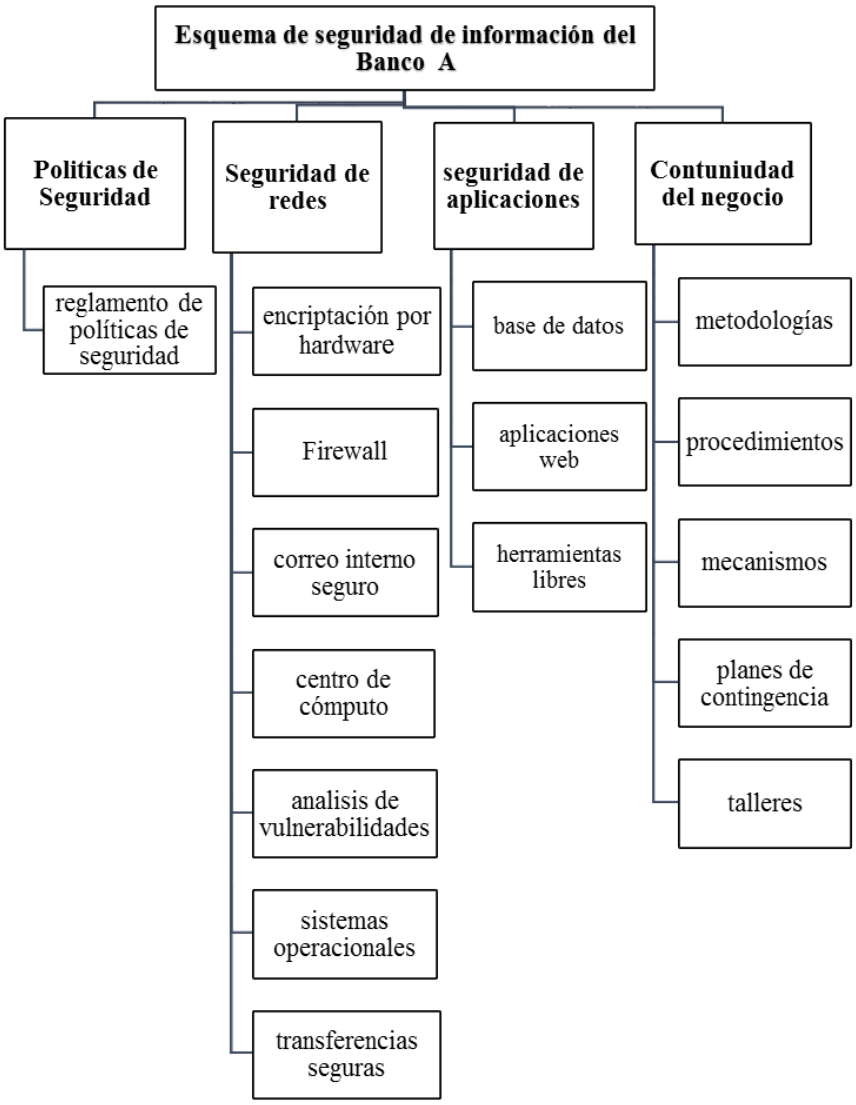
El trabajo realizado analiza y estudia las actividades realizadas por el departamento de tecnología y comunicaciones respecto a la seguridad que se aplica en el almacenamiento de datos confidenciales del titular de tarjeta, para contribuir con los objetivos establecidos y la continuidad del negocio de tarjetas de pago.

6.7 Metodología

6.7.1 Modelo Operativo

El esquema actual que se presenta, es resultado y levantamiento de información que fue aplicado al personal del departamento de sistemas y comunicaciones se detallan de la siguiente manera:

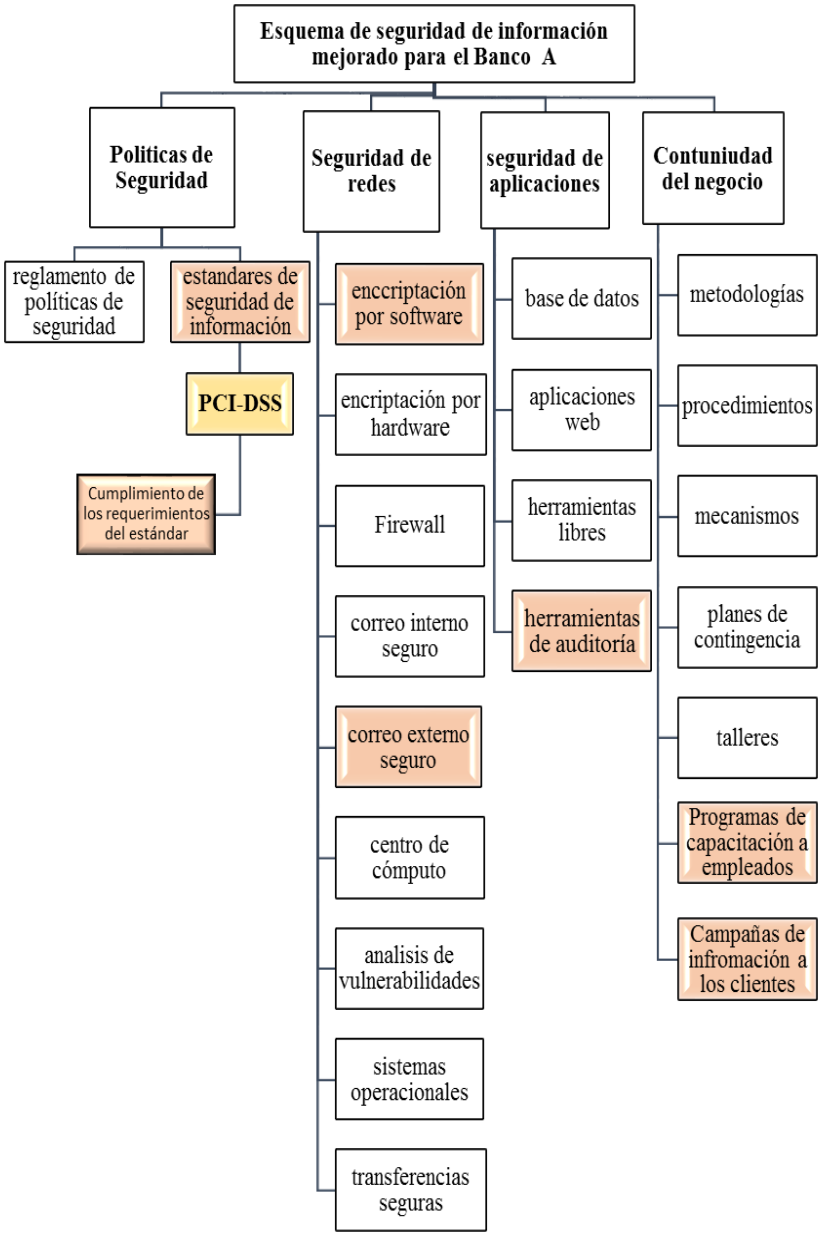
Figura 30. Esquema de seguridad de información del Banco A.



Elaborado por: personal de área del departamento de sistemas y comunicaciones
Fuente: Información proporcionada por el Banco A

Se aconseja al banco A restructurar, el esquema de seguridad, para una mejor definición de los procedimientos de la siguiente forma:

Figura 31. Esquema de seguridad de información mejorado para el Banco A.



Elaborado por: Autores.
Fuente: Información proporcionada por el Banco A

6.8 Administración

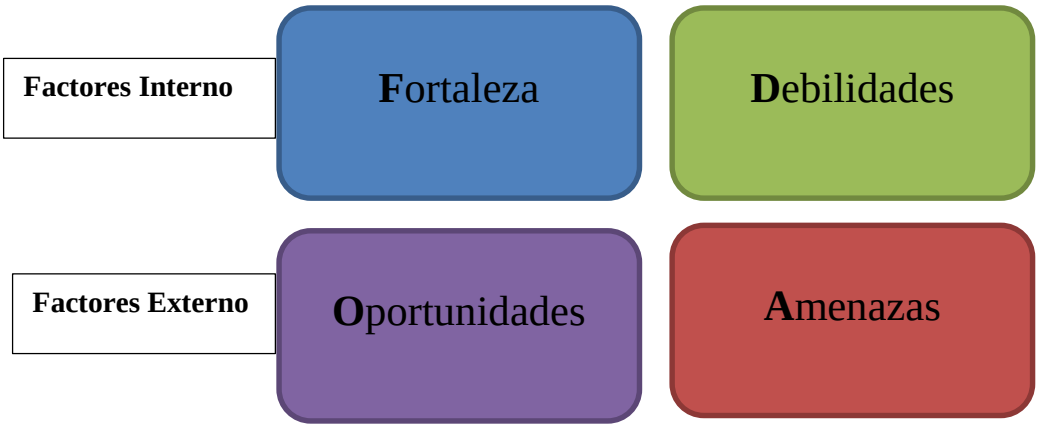
La presente propuesta será administrada por:

- El jefe del departamento de tecnología y comunicaciones.
- Las proponentes: Andrea Mejía – Alexandra Calle

6.9 Descripción de la Propuesta

Tomando en consideración los resultados obtenidos por medio de la encuesta realizada al personal del Departamento de Tecnología de la entidad Bancaria A, se propone realizar las siguientes actividades:

- **Realizar un análisis FODA**
- **Análisis del cumplimiento del Plan de Acción**
- **Determinación de Estrategias a seguir para mejorar las normas de seguridad de la información en la entidad Bancaria.**
- **Implementación de Requerimientos para la adecuación y aseguramiento**



Elaborado por: Autores.
Fuente: Seguridad de la información

Tomando en consideración cada uno de estos factores, existe la posibilidad de realizar con mayor y mejor resultados un análisis pare el cumplimiento del Plan de Acción destinado al aseguramiento de la red, cuya finalidad se centra en la reducción del fraude relacionado con las tarjetas de crédito y el aumento de la seguridad de datos basados en el Estándar PCI-DSS.

Análisis FODA de la Entidad Bancaria A

FORTALEZAS	**OPORTUNIDADES**
Buen posicionamiento en el Mercado Nacional	Identificar riesgos que afecten la seguridad de la información de los tarjetahabientes
Goza de la confianza de los clientes, socios de negocios y accionistas	Facilita el Gobierno corporativo de TI
Fluidez económica garantizada	Incrementar la confianza de los clientes, socios de negocios y accionistas
Personal de sistemas capacitados y comprometidos	Proteger la imagen y reputación de la Entidad Financiera
DEBILIDADES	**AMENAZAS**
Carga laboral en el personal del Departamento de Sistemas	Elevación de precios en los equipos de tecnología
Limitaciones en el presupuesto para la adquisición de nuevas herramientas de control	Dificultad financiera del banco A
Burocracia interna para solicitar personal y recurso tecnológico eficiente	Ataque físico a los equipos informáticos
Escaza atención a las necesidades del Departamento de Sistemas	Personal de sistemas no capacitado

Para llegar a optimizar las seguridades dentro de los estándares establecidos en la Norma PCI-DSS es necesario realizar posterior al análisis FODA un flujo de organización, donde se determine cada una de las fases o puntos en la cadena de valor donde se transmite, procesa o almacena información proveniente de las tarjetas de créditos, tomando en consideración que este tipo de operaciones relativamente son parte de la actividad económica y transaccional de la entidad Bancaria en estudio, llegando de esta forma a definir un que cumpla a cabalidad con PCI-DSS.

Figura 32. Fases

Elaborado por: Autores.
Fuente: Pci- Dss

Para el éxito de la aplicación de la Guía de Auditoria de Sistemas que permita evaluar el control interno de una Institución Financiera basado en los Estándares PCI-DSS en la Seguridad de la Información", es necesario a correcta ejecución de una serie de fases que garantizan el éxito del proceso de auditoría.

EL Análisis del estado de Cumplimiento

Para realizar un correcto proceso de auditoría se precisa contar con el personal idóneo, el mismo que tenga pleno conocimiento sobre los estándares de seguridad, con quienes se desarrollará un cronograma planteando el trabajo preliminar y el mecanismo con el cual se va a llevar a cabo dicho proceso.

Es preciso conocer cómo afecta los PCI-DSS a los Clientes y de qué manera la entidad Bancaria lleva la información de las tarjetas de créditos. A continuación se revisa el

estado actual del cumplimiento de los requisitos PCI-DSS, detallar en lo mejor posible el cumplimiento al mínimo imprescindible, se trata de reducir al máximo los costos innecesarios de implantación y mantenimiento de programas de seguridad, toda esta fase se lo debe realizar en el menor tiempo posible.

Valoración de riesgos y prioridades de acciones

Dentro de esta etapa es necesario valorar cada uno de los riesgos sobre el entorno de protección definido en el Entorno de Cumplimiento, basándose en el diagnóstico realizado sobre los requerimientos PCI-DSS y así establecer los puntos o debilidades con los que cuenta la organización, asumiendo las prioridades y subsanación de dichos riesgos, atacando a los mismo de manera inmediata y oportuna, entrando nuevamente en los lineamientos que exige los estándares PCI-DSS, este tipo de proceso se lo realiza mediante el documento PCI-DSS Prioritezed Approach, encargado de definir una metodología de cómo implementar un PCI-DSS minimizando al máximo el riesgo de los compromisos de datos, basados en 6 fases.

1. Eliminación de información relativa a la autenticación y limitante para la retención de la misma.
2. Protección del perímetro, intranet y redes Wireless
3. Utilidad de aplicaciones seguras
4. Monitoreo y control de acceso a las aplicaciones.
5. Protección de la información del titular de la tarjeta.
6. Fiel cumplimiento de los demás requerimientos.

Programa de Cumplimiento

Mediante esta fase se llega a determinar las estrategias a seguir por la Organización, los mismos que lo direccionan al cumplimiento de los requerimientos PCI-DSS, disminuyendo los riesgos y vulnerabilidades identificadas, orientando la inversión en seguridad dentro de la entidad Bancaria, por lo que es necesario definir las normas de control y aseguramiento de la información basados en las normas PCI-DSS y lo establecido por la norma ISO/IEC 27001:2013, dando paso a la certificación de Sistemas de Gestión Segura de la Información (SGGI).

Estrategias a utilizar para mejorar el control interno de la información basada en los Estándares PCI-DSS

Estrategias para una Red Segura

- Realizar un diagrama de la estructura de la Red.
- Determinar el tiempo de vida útil de los equipos de la red
- Instalación y mantenimiento de cortafuegos, cuya configuración permita proteger los datos de los propietarios de las tarjetas.
- Cambiar las contraseñas de seguridad proporcionado por los proveedores de manera constante.

Estrategias de protección de datos de los propietarios de las tarjetas

- Cifrado de datos e información considerada confidencial que se transmite por medio de las redes públicas abiertas.
- Almacenamiento seguro de la información de los propietarios de los datos.
- Detección de la IP de del equipo de entrada de información del dueño de la tarjeta.

Estrategias de Vulnerabilidades

- Usar y actualizar de forma frecuente el software de vulnerabilidades que por lo general provienen de virus informáticos.
- Implementación y desarrollo de sistemas seguros, así como de aplicaciones que permitan un verdadero control de auditoría interno.

Estrategias de Accesos

- Establecer parámetros internos para la solicitud de información confidencial de los tarjetahabientes.
- Establecer roles y parámetros para el acceso de la misma.
- Establecer niveles de seguridad en el personal de sistema para la

actualización y mantenimiento de los equipos y sistemas informáticos.

- Asignar un identificador único a cada miembro de la entidad Bancaria para el acceso de la información.
- Dar a conocer las responsabilidades de la asignación del identificador, la misma que no es transferible.
- Eliminar o restringir el acceso físico a la información de los dueños de las tarjetas.

Estrategias de monitoreo

- Realizar un seguimiento muy frecuente sobre el acceso a los recursos de la red.
- Realizar un seguimiento muy frecuente sobre el acceso a la información de los datos del dueño de la tarjeta por medio del identificador de usuario.
- Limitar o restringir modificaciones internas de información, solo previa autorización y justificativo de la misma.
- Testear de manera regular los sistemas y procesos de seguridad.

Estrategias de Políticas de Seguridad

- Elaborar Políticas de Seguridad que se acoplen a las necesidades y modelos del negocio en el área informática, independiente a los procesos y actividades económicas de las otras áreas.
- Socializar las Políticas de Seguridades así como las responsabilidades y consecuencias del mal manejo de la información en todo el personal que labora en la entidad Bancaria.
- Realizar reportes de las actividades por usuario sobre el manejo de los recursos de la red y la seguridad e integridad de la información.

6.10 Lineamientos para evaluar la propuesta

La propuesta será evaluada, tomando en consideración el mejoramiento de los sistemas de seguridad y manejo de la información de los tarjetahabientes, así como la optimización de los reportes y controles de actividades de los usuarios asignados para el acceso y manejo de datos confidenciales, recursos de redes y solicitud de información personal del dueño de la tarjeta.

De la misma forma el constante monitoreo de los sistemas de redes y seguridades internas y externas de la información, como el cambio de los equipos que han cumplido con su vida útil, acoplando nuevos modelos apegados fiel cumplimento de los Estándares PCI-DSS. Mejora en el nivel de conocimiento del personal de la Institución Financiera sobre las Políticas de Seguridad de la Información.

BIBLIOGRAFÍA

7812-2:2007, ISO/IEC. (s.f.). *Identification Card.* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:7812:-2:ed-3:v1:en

BANCO DE GUAYAQUIL. (9 de 2 de 2012). *BANCO DE GUAYAQUIL PRIMER BANCO EN RECIBIR CERTIFICACIÓN PCI-DSS*. Recuperado el 10 de 11 de 2014, de BANCO DE GUAYAQUIL PRIMER BANCO EN RECIBIR CERTIFICACIÓN PCI-DSS: http://www.bancoguayaquil.com/

Blaustein, L. (5 de 11 de 2014). *TechTarget*. (TechTarget) Recuperado el 15 de 01 de 2015, de TechTarget: http://searchdatacenter.techtarget.com/es/cronica/Como-mejorar-la-seguridad-con-una-adecuada-segmentacion-de-redes

COUNCIL, PCI SECURITY. (OCTUBRE de 2010). *Glosario de Terminos V2.0.* Recuperado el 5 de Enero de 2015, de Glosario de Terminos V2.0: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI%20Glossary.pdf

COUNCIL, PCI SECURITY. (Enero de 2014). *Glosario de Terminos V3.0.* Recuperado el 16 de Febrero de 2015, de Glosario de Terminos V3.0: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3_Glossary_ES-LA.pdf

CVVNumber. (2015). Tarjetas de Credito y Debito CVV. *Tarjetas de Credito y Debito CVV*, pág. https://www.cvvnumber.com/.

Infomation Quality. (2013). *IQ Seguridad en pagos Electronicos*. Recuperado el 12 de 2 de 2015, de IQ Seguridad en pagos Electronicos: http://www.iqcol.com/

LVC. (07 de 05 de 2013). Pacificard da seguridad a sus clientes. *Pacificard da seguridad a sus clientes*. Obtenido de Certificacion PCI-DSS.

Maria, M. (28 de 08 de 2010). *Fraudes en Telecomunicaciones.* Recuperado el 15 de 02 de 2015, de Fraudes en Telecomunicaciones: http://www.supertel.gob.ec/pdf/libro_fraude_telecomunicaciones.pdf

PCI Security Council. (Octubre de 2010). *Requisitos y procedimientos de evaluación de Seguridad PCI-DSS v2.0.* Recuperado el 26 de noviembre de 2014, de Requisitos y procedimientos de evaluación de Seguridad PCI-DSS v2.0: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/pci_pa_dss_v2-0.pdf

PCI Security Council. (Noviembre de 2013). *Requisitos y procedimientos de evaluación de Seguridad PCI-DSS v3.0.* Recuperado el 19 de Febrero de

2015, de Requisitos y procedimientos de evaluación de Seguridad PCI-DSS v3.0: https://es.pcisecuritystandards.org/

PCI Security Council. (Noviembre de 2013). *Resumen de los Cambios de la V2.0 a v3.0.* Recuperado el 12 de 02 de 2015, de PCI STANDAR & DOCUMENTS: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3_Summary_of_Changes.pdf

Rider, J. (4 de 8 de 2011). *¿Quién tiene que cumplir PCI-DSS? ¿Cuáles son las obligaciones?* Recuperado el 4 de 1 de 2015, de ¿Quién tiene que cumplir PCI-DSS? ¿Cuáles son las obligaciones?: http://cumplirpci.blogspot.com/

Superintendencia de Bancos del Ecuador. (2012). *Evite Fraudes Electronicos*. Recuperado el 04 de 03 de 2015, de Evite Fraudes Electronicos: http://portaldelusuario.sbs.gob.ec/contenido.php?id_contenido=33

Superintendencia de Bancos del Ecuador. (26 de abril de 2012). *Resolución JB-2012-2148.* Recuperado el 05 de 03 de 2015, de Resolución JB-2012-2148: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

ANEXOS

ANEXO 1: GLOSARIO PCI-DSS

Autenticación: Proceso para verificar la identidad de un individuo, dispositivo o proceso. Por lo general, la autenticación ocurre a través del uso de uno o más factores de autenticación, tales como:

- ✓ Algo que el usuario sepa, como una contraseña o frase de seguridad.
- ✓ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente.
- ✓ Algo que el usuario sea, como un rasgo biométrico Credenciales de autenticación.
- ✓ Combinación del ID de usuario o ID de la cuenta más el (los) factor(es) utilizado(s) para autenticar a un individuo, dispositivo o proceso.

Autorización: Otorgamiento de derechos de acceso u otros derechos similares a un usuario, programa o proceso. En cuanto a las redes, la autorización define lo que un individuo o programa puede hacer después de un proceso de autenticación satisfactorio. En lo que se refiere a la autorización de una transacción con tarjeta de pago, ésta ocurre cuando un comerciante recibe la a probación de la transacción después de que el adquirente valide la transacción con el emisor/procesador.

Titular de tarjeta: Cliente consumidor o no consumidor para el que se emite la tarjeta de pago, o cualquier individuo autorizado para utilizar una tarjeta de pago.

Datos del titular de la tarjeta: Los datos del titular de la tarjeta contienen, como mínimo, el PAN completo. Es posible que los datos del titular de la tarjeta también incluyan el PAN completo más alguno de los siguientes datos: nombre del titular de la tarjeta, fecha de vencimiento y/o código de servicio.

Entorno de datos de titulares de tarjetas: Las personas, los procesos y la tecnología que almacenan, procesan o transmiten datos de titulares de tarjetas o datos

confidenciales de autenticación, incluidos todos los componentes del sistema conectados.

La siguiente lista especifica los términos según la marca de tarjeta:

CAV – Card Authentication Value (valor de autenticación de la tarjeta) (tarjetas de pago JCB)

CVC – Card Validation Code (código de validación de la tarjeta) (tarjetas de pago MasterCard)

CVV – Card Verification Value (valor de verificación de la tarjeta) (tarjetas de pago Visa y Discover)

CSC – Card Security Code (código de seguridad de la tarjeta) (tarjetas de pago American Express

La siguiente lista especifica los términos según la marca de la tarjeta:

CID – Card Identification Number (número de identificación de la tarjeta) (tarjetas de pago American Express y Discover)

CAV2 – Card Authentication Value 2 (valor de autenticación de la tarjeta 2) (tarjetas de pago JCB)

CVC2 – Card Validation Code 2 (código de validación de la tarjeta 2) (tarjetas de pago MasterCard)

CVV2 – Card Verification Value 2 (valor de verificación de la tarjeta 2) (tarjetas de pago Visa)

Cifrado de bases de datos a nivel de columna: Técnica o tecnología (ya sea software o hardware) para cifrar el contenido de una columna específica de una base de datos y no todo el contenido de toda la base de datos. Consulte también Cifrado de disco o Cifrado a nivel de archivo.

Riesgo: También denominado “riesgo de datos” o “violación de datos”. Intrusión en un sistema de computadoras en la cual se sospecha una divulgación, un robo, una modificación o la destrucción no autorizada de datos del titular de la tarjeta.

Consola: Pantalla o teclado que permite obtener acceso al servidor, equipo mainframe u otro tipo de sistema y controlarlo dentro de un entorno de red.

Consumidor: Persona que compra bienes, servicios o ambos.

Criptografía: Disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.

Período de cifrado: Lapso de tiempo durante el cual se puede utilizar una clave criptográfica para su propósito definido basándose en, por ejemplo, período de tiempo definido y/o la cantidad de texto cifrado producido, y según las mejores prácticas y directrices de la industria.

Base de datos: Formato estructurado que permite organizar y mantener información de fácil recuperación. Algunos ejemplos simples de base de datos son las tablas y las hojas de cálculo.

Administrador de bases de datos: Denominado también "DBA", se refiere al responsable de administrar bases de datos.

Cuentas predeterminadas: Cuenta de inicio de sesión que se encuentra predefinida en un sistema, aplicación o dispositivo que permite obtener acceso por primera vez al momento en que el sistema comienza a funcionar. El sistema también puede generar cuentas predeterminadas adicionales como parte del proceso de instalación.

Contraseña predeterminada: Contraseña de las cuentas de usuario, servicio o administración de sistemas predefinidas en un sistema, aplicación o dispositivo asociado con la cuenta predeterminada. Las contraseñas y cuentas predeterminadas son de dominio público y, en consecuencia, es fácil averiguarlas.

Destrucción magnética: También denominada "destrucción magnética de disco". Proceso o técnica que desmagnetiza un disco para destruir permanentemente toda la información almacenada en éste.

Cifrado de disco: Técnica o tecnología (ya sea de software o hardware) que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro

o una unidad flash). También se utiliza el cifrado a nivel de archivo y el cifrado de bases de datos a nivel de columna para cifrar el contenido de archivos o columnas específicas.

DMZ: Abreviatura de "demilitarized zone" (zona desmilitarizada). Subred física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización. La DMZ agrega una capa de seguridad de red adicional entre Internet y la red interna de una organización, de modo que las partes externas sólo tengan conexiones directas a los dispositivos de la DMZ y no a toda la red interna.

DNS Acrónimo de "Domain Name System": (sistema de nombre de dominio) o "domain name server" (servidor de nombre de dominio). Sistema que almacena información relacionada con nombres de dominio en una base de datos distribuida en redes, como Internet.

DSS: Acrónimo de "Data Security Standard" (norma de seguridad de datos), también denominada "PCI-DSS".

Control dual: Proceso que consiste en utilizar dos o más entidades distintas (por lo general, personas) de manera coordinada para proteger funciones o información confidenciales. Ambas entidades son igualmente responsables de la protección física de los materiales que intervienen en transacciones vulnerables. Ninguna persona tiene permitido obtener acceso a o utilizar estos materiales (por ejemplo, la clave criptográfica). Para generar, transferir, cargar, almacenar y recuperar manualmente una clave, el proceso de control dual requiere que se divida el conocimiento de la clave entre las entidades.

ECC: Acrónimo de "Elliptic Curve Cryptography" (criptografía de curva elíptica). Método de criptografía de clave pública basado en curvas elípticas sobre campos finitos.

Filtrado de egreso: Método que permite filtrar el tráfico saliente de una red, de modo que sólo el tráfico explícitamente autorizado pueda salir de la red.

Cifrado: Proceso para convertir información en un formato ilegible, a excepción de los titulares de una clave criptográfica específica. El cifrado se utiliza para proteger la

información entre el proceso de cifrado y el proceso de descifrado (lo contrario del cifrado) de la divulgación no autorizada.

Algoritmo de cifrado: Secuencia de instrucciones matemáticas usadas para transformar textos o datos no cifrados en textos o datos cifrados y viceversa. Consulte

Entidad: Término utilizado para representar a la corporación, organización o negocio bajo una revisión de las PCI-DSS.

Supervisión de la Integridad de archivos: Técnica o tecnología utilizada para supervisar archivos o registros a fin de detectar si se modificaron. Si se modifican archivos o registros críticos, se debería enviar mensajes de alerta al personal de seguridad apropiado.

Cifrado a nivel de archivo: Técnica o tecnología (ya sea software o hardware) para cifrar todo el contenido de archivos específicos.

FIPS: Acrónimo de "Federal Information Processing Standards" (normas de procesamiento de información federal de los EE. UU). Normas aceptadas públicamente por el gobierno federal de los EE. UU, a disposición también de agencias no gubernamentales y contratistas.

Firewall: Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tráfico de computadoras entre redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios.

Herramientas forenses: También se denomina "informática forense". Cuando se trata de la seguridad de la información, se refiere a la aplicación de herramientas de investigación y técnicas de análisis para recolectar evidencia a partir de recursos informáticos a fin de determinar la causa del riesgo de los datos.

FTP Acrónimo de "File Transfer Protocol": (protocolo de transferencia de archivos). Protocolo de red que se utiliza para transferir datos de una computadora a otra mediante un red pública, como Internet. En general, se considera que FTP es un protocolo inseguro, porque permite enviar contraseñas y contenido de archivos sin protección y en texto simple. El protocolo FTP puede implementarse con seguridad mediante SSH u otra tecnología.

GPRS: Acrónimo de "General Packet Radio Service" (servicio de radio paquete general). Servicio de datos portátil disponible para los usuarios de teléfonos móviles GSM. Reconocido por el uso eficaz de un ancho de banda limitado. Ideales para enviar y recibir pequeños paquetes de datos, como correos electrónicos y para navegar en Internet.

GSM: Acrónimo de "Global System for Mobile Communications" (sistema global de comunicaciones móviles). Norma ampliamente difundida para teléfonos móviles y redes. La ubicuidad de la norma GSM convierte el acceso de llamada itinerante o "roaming" a nivel internacional en algo muy común entre los operadores de telefonía inalámbrica, lo que permite a los suscriptores utilizar sus teléfonos en distintos lugares del mundo.

Hashing: Proceso que vuelve ilegibles los datos de titulares de tarjetas convirtiendo los datos en un ññ´¿ de mensaje de longitud fija mediante la Criptografía sólida. El hashing es una función (matemática) en la cual un algoritmo conocido toma un mensaje de longitud arbitraria como entrada y produce un resultado de longitud fija (generalmente denominado "código hash" o "resumen de mensaje"). Una función hash debe tener las siguientes propiedades: (1) Que no se pueda determinar informáticamente la entrada original si sólo se tiene el código hash, (2) Que no se puedan hallar informáticamente dos entradas que generen el mismo código hash. En el contexto de las PCI-DSS, la función hash se debe aplicar a todo el PAN para que se considere que el código hash es ilegible. Se recomienda que los datos de titulares de tarjetas en valores hash incluyan un valor de sal como entrada a la función de hashing.

Host: Computadora principal donde reside el software informático.

Proveedor de hosting: Ofrece diferentes servicios a comerciantes y otros proveedores de servicios. Los servicios van de simples a complejos: desde un espacio compartido en un servidor hasta una completa gama de opciones para el "carrito de compras"; desde aplicaciones de pago hasta conexiones con pasarelas y procesadores de pago; y para proveer servicio de hosting dedicado sólo a un cliente por servidor. Es posible que el proveedor de hosting sea un proveedor de hosting compartido, encargado de prestar servicio a diferentes entidades en un solo servidor.

HTTP: Acrónimo de "hypertext transfer protocol" (protocolo de transferencia de hipertexto). Protocolo abierto de Internet que permite transferir o transmitir información en la World Wide Web.

HTTPS: Acrónimo de "hypertext transfer protocol over secure socket layer" (protocolo de transferencia de hipertexto a través de una capa de conexión segura). HTTP seguro que proporciona autenticación y comunicación cifrada en la World Wide Web diseñado para comunicaciones que dependen de la seguridad, tales como los inicios de sesión basados en la web.

Hipervisor Software o firmware: responsable de prestar servicios de hosting a máquinas virtuales y administrarlas. En cuanto a las PCI-DSS, el componente del sistema hipervisor también incluye el VMM, virtual machine monitor (supervisor de máquinas virtuales).

ID: Identificador correspondiente a un usuario o una aplicación particular.

IDS: Acrónimo de "intrusion detection system" (sistema de detección de intrusiones). Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad detectado.

IETF: Acrónimo de "Internet Engineering Task Force" (grupo de trabajo de ingeniería en Internet). Comunidad internacional abierta y extensa de diseñadores de redes, operadores, proveedores e investigadores que trabajan en el desarrollo de la arquitectura de Internet y se ocupan de su correcto funcionamiento. El IETF no exige la acreditación de membresías y está abierto a cualquier persona interesada.

Token de índice: Token criptográfico que, basado en un índice dado para un valor imprevisible, reemplaza el PAN.

Seguridad de la información: Protección de la información que garantiza la confidencialidad, integridad y disponibilidad.

Sistema de información: Conjunto específico de recursos de datos estructurados organizados para recolectar, procesar, mantener, usar, compartir, diseminar o disponer de la información.

Filtrado de ingreso: Método que permite filtrar el tráfico entrante de una red, de modo que sólo el tráfico explícitamente autorizado pueda ingresar a la red.

Protocolo/Servicio/Puerto no seguros: Un protocolo, servicio o puerto que produce preocupación en cuanto a la seguridad debido a la falta de controles de confidencialidad y/o integridad. Estas preocupaciones relacionadas con la seguridad afectan a los servicios, protocolos o puertos que transmiten datos y credenciales de autenticación (como contraseñas o frases de seguridad de texto simple en Internet), o son fáciles de explotar si se configuran incorrectamente o de forma predeterminada. Entre los servicios, protocolos o puertos no seguros se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP.

IP: Acrónimo de "internet protocol" (protocolo de Internet). Protocolo de capas de red que contiene información sobre direcciones y algunos datos de control, y permite el ruteo de paquetes. IP es el protocolo primario de capas de red en la suite de protocolos de Internet.

Dirección IP: También denominada "dirección de protocolo de Internet". Código numérico que identifica exclusivamente una computadora en Internet.

Falsificación de dirección IP: Técnica de ataque que utiliza una persona malintencionada para obtener acceso no autorizado a computadoras. La persona malintencionada envía mensajes engañosos a una computadora. Los mensajes tienen una dirección IP que indica que el mensaje proviene de un host de confianza.

IPS: Acrónimo de "intrusion prevention system" (sistema de prevención de intrusiones). El IPS va un paso más allá que el IDS y bloquea el intento de intrusión.

IPSEC: Abreviatura de "Internet Protocol Security" (protocolo de seguridad de Internet). Norma para asegurar las comunicaciones IP mediante el cifrado y/o la autenticación de todos los paquetes IP. IPSEC brinda seguridad en la capa de red.

ISO: Acrónimo de "International Organization for Standardization" (Organización Internacional de Normalización). Organización no gubernamental formada por una red

de institutos nacionales de normalización pertenecientes a más de 150 países, con un miembro representante por país y una secretaría central, en Ginebra, Suiza, que se encarga de coordinar el sistema.

Emisor: Entidad que emite tarjetas de pago o realiza, facilita o respalda servicios de emisión incluidos, a modo de ejemplo, bancos y procesadores emisores. También denominado "banco emisor" o "instituciones financieras emisoras".

Servicios de emisión: Entre los ejemplos de servicios de emisión se pueden incluir, a modo de ejemplo, la autorización y la personalización de tarjetas.

Clave: En criptografía, una clave es un valor que determina el resultado de un algoritmo de cifrado al transformar texto simple en texto cifrado. En general, la extensión de una clave determina la dificultad para descifrar el texto de un determinado mensaje.

Administración de claves: En criptografía, se refiere al conjunto de procesos y mecanismos que respaldan el establecimiento y mantenimiento de las claves, así como el reemplazo de claves anteriores por nuevas claves, según sea necesario.

LAN: Acrónimo de "local area network" (red de área local). Grupo de computadoras y/u otros dispositivos que comparten una línea de comunicaciones común, generalmente, en un edificio o grupo de edificios.

LDAP: Acrónimo de "Lightweight Directory Access Protocol" (protocolo ligero de acceso directo). Repositorio de datos para la autenticación y autorización destinado a las consultas y modificaciones relativas a permisos de usuario y al otorgamiento de derechos de acceso a recursos protegidos.

MAC: Acrónimo de "message authentication code" (código de autenticación de mensajes).

Dirección MAC: Abreviatura de "media access control address" (dirección de control de acceso a medios). Valor único de identificación que el fabricante asigna a los adaptadores de red y a las tarjetas de interfaz de red.

Datos de la banda magnética también denominados "datos de pistas": Datos codificados en la banda magnética o el chip que se utilizan para la autenticación y/o

autorización durante las transacciones de pago. Puede ser la imagen de la banda magnética de un chip o los datos de la pista 1 y/o pista 2 de la banda magnética.

Mainframe: Computadoras diseñadas para trabajar con grandes volúmenes de entrada y salida de datos y para enfatizar el rendimiento informático. Los sistemas mainframe pueden ejecutar varios sistemas operativos, por lo que parece que estuvieran operando como múltiples computadoras. Muchos sistemas heredados presentan un diseño de mainframe.

Software malicioso o malware: Software desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema.

Algunos ejemplos son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.

Ocultamiento: En el contexto de las PCI-DSS, se refiere al método para ocultar un segmento de los datos cuando se muestran o imprimen. El ocultamiento se utiliza cuando no existe un requisito por parte del negocio de ver el PAN completo. El ocultamiento se relaciona con la protección del PAN cuando se muestra o imprime.

Comerciante: En lo que concierne a las PCI-DSS, comerciante se define como toda entidad que acepta tarjetas de pago con el logotipo de cualquiera de los cinco miembros del PCI SSC (American Express, Discover, JCB, MasterCard o Visa) como forma de pago por bienes y servicios.

Supervisión: Uso de sistemas o procesos que constantemente vigilan los recursos de computadoras o redes a efectos de alertar al personal en caso de interrupciones, alarmas u otros eventos predefinidos.

MPLS Acrónimo de “multi protocol label switching” (conmutación multi-protocolo mediante etiquetas). Mecanismo de red o telecomunicaciones diseñado para conectar un grupo de redes basadas en la conmutación de paquetes.

NAT Acrónimo de “network address translation” (traducción de direcciones de red). Llamada simulación de red o simulación IP. Cambio de la dirección IP utilizada dentro de una red por una dirección IP distinta conocida dentro de otra red.

Red: Dos o más computadoras interconectadas a través de un medio físico o inalámbrico.

Administrador de red: Personal responsable de administrar la red dentro de una entidad. Entre las responsabilidades generalmente se incluyen, a modo de ejemplo, la seguridad, las instalaciones, las actualizaciones, el mantenimiento y la supervisión de la actividad de la red.

Componentes de red: Los componentes de la red incluyen, a modo de ejemplo, firewalls, conmutadores, routers, puntos de acceso inalámbrico, aplicaciones de red y otras aplicaciones de seguridad.

Análisis de seguridad de la red: Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas.

Segmentación de red: La segmentación de red separa componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta de sistemas que no lo hacen.

NIST Acrónimo de "National Institute of Standards and Technology" (Instituto Nacional de Normas y Tecnología): Agencia federal no regulatoria dependiente de la Administración Tecnológica del Departamento de Comercio de los Estados Unidos. Su misión es promover la innovación estadounidense y la competitividad industrial mediante la promoción de medidas de ciencia, normas y tecnologías que mejoren la estabilidad económica y la calidad de vida.

NMAP: Software para el análisis de riesgos de seguridad encargado de delinear redes e identificar puertos abiertos en los recursos de red.

Usuarios no consumidores: son todas las personas, con excepción de los titulares de tarjetas, que tengan acceso a los componentes de sistema, entre los cual s se incluyen empleados, administradores y terceros.

NTP: Acrónimo de "network time protocol" (Protocolo de tiempo de red).

Protocolo usado para sincronizar los relojes de sistemas informáticos, dispositivos de red y otros componentes del sistema.

Productos estándar: Descripción de productos listos para usar comercializados como bienes no personalizadas o específicamente diseñadas para un cliente o usuario.

Sistema operativo/OS: Software de un sistema de computadoras a cargo de compartir recursos informáticos y administrar y coordinar todas las actividades informáticas.

Algunos ejemplos de sistemas operativos incluyen Microsoft Windows,

Mac OS, Linux y Unix.

OWASP: Acrónimo de "Open Web Application Security Project" (Guía para proyectos de seguridad de aplicaciones web abiertas). Es una organización sin fines de lucro especializada en mejorar la seguridad del software de aplicación. OWASP mantiene una lista con las vulnerabilidades más críticas de las aplicaciones web. (Consulte http://www.owasp.org).

PA-QSA: Acrónimo de "Payment Application Qualified Security Assessor" (Asesor de seguridad certificado para las aplicaciones de pago), una empresa calificada por las PCI SSC para realizar evaluaciones de aplicaciones de pago de acuerdo con las PA-DSS.

PCI-DSS: Acrónimo de "Payment Card Industry Data Security Standard" (Norma de seguridad de datos de la industria de tarjetas de pago).

PIN: Acrónimo de "personal identification number" (número de identificación personal). Contraseña numérica secreta que conocen solo el usuario y un sistema para autenticar al usuario en el sistema. El usuario tan solo obtiene acceso si su PIN coincide con el PIN del sistema. Los PIN más comunes se utilizan en las transacciones de adelanto de efectivo y las ATM. Otro tipo de PIN es el que utilizan las tarjetas con chip de tipo EMV, en las que el PIN reemplaza la firma del titular de la tarjeta.

QSA: Acrónimo de "Qualified Security Assessor" (Asesor de Seguridad Certificado). Los QSA están calificados por las PCI SSC para realizar evaluaciones en el lugar.

Política: Normas vigentes para toda la organización que reglamentan el uso aceptable de los recursos informáticos, las prácticas de seguridad y el desarrollo guiado de procedimientos operacionales

Política de seguridad: Conjunto de leyes, reglamentos y prácticas que regulan el modo en una organización administra, protege y distribuye información confidencial.

Flujo de datos de una Tarjeta: Hace referencia a la trayectoria del requerimiento transaccional que se genera con una tarjeta de pago hasta su aprobación considerando la captura de los datos cada uno de los puntos implicados.

Housing: se entiende como alojamiento web, implica el alquiler de un espacio físico para que el cliente o empresa coloque en ese lugar su servidor.

Datacenter: se conoce generalmente como centro de cómputo es el lugar donde se encuentran ubicados los recursos y los equipos esenciales para el procesamiento de información de una organización.

Programas de lealtad: Se define como una estrategia de retención de clientes, mediante la cual se otorga beneficios considerables a los usuarios que utilizan frecuentemente tarjetas de pago como por ejemplo: catálogos de canje, descuentos, viajes. Las grandes industrias de tarjetas de crédito mantienen programas de lealtad como American Express con “Membership Rewards” y Diners Club con “Club Rewards”.

VLANs: (Virtual Local Area Network) Es la segmentación de una red física de área local, en varias redes lógicas independientes.

Redes Planas: Es una red de arquitectura simplificada, que permite flexibilidad y reorganización de los equipos.

Back office active: Back Office Activo (ABO) es un proveedor de productos de proveedores de servicios mayoristas y servicios para los despliegues de telefonía IP. Como ventanilla única de soluciones de transporte, ABO ofrece un único, de alta calidad conjunto de ofrendas a los proveedores de VoIP emergentes y portadores de voz establecidos. Su amplia cartera integrada incluye Hosted PBX, E911 para VoIP, originación y terminación a nivel nacional, CNAM, 411, y el directorio a nivel nacional los servicios de listado.

ANEXO 2: Cuestionario de autoevaluación y Declaración de cumplimiento del Estándar de Seguridad PCI-DSS.

DESARROLLAR Y MANTENER UNA RED SEGURA.

Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos.

	Respuesta a la Pregunta de PCI DSS:	Sí	No	Especial
1.1	¿Incluyen las normas de configuración del firewall y router establecidas lo siguiente?			
1.1.1	¿Existe un proceso formal para aprobar y probar todos los cambios y las conexiones externas de red en la configuración de los firewalls y los routers?	☐	☐	
1.1.2	(a) ¿Existe un diagrama de red actualizado (por ejemplo, uno que muestre los flujos de los datos de los titulares de tarjetas en la red) que documente todas las conexiones a los datos de los titulares de tarjetas, incluidas todas las redes inalámbricas?	☐	☐	
	(b) ¿Se mantiene actualizado el diagrama?	☐	☐	
1.1.3	(a) ¿Incluyen las normas de configuración requisitos para tener un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de la red interna?	☐	☐	
	(b) ¿Se corresponde el diagrama actual de la red con las normas de configuración de firewalls?	☐	☐	
1.1.4	¿Incluyen las normas de configuración del firewall y router una descripción de grupos, funciones y responsabilidades para una	☐	☐	

	administración lógica de los componentes de la red?		
1.1.5	(a) ¿Incluyen las normas de configuración de firewalls y routers una lista documentada de los servicios, protocolos y puertos necesarios para el negocio (por ejemplo, el protocolo de transferencia de hipertexto (HTTP) y los protocolos Protocolo de Capa de Conexión Segura (SSL), Secure Shell (SSH) y Red Privada Virtual (VPN).	☐	☐
	(b) ¿Son necesarios todos los servicios, protocolos y puertos no seguros; además, se documentaron e implementaron características de seguridad para cada uno de ellos? Nota: Entre los servicios, protocolos o puertos no seguros se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP.	☐	☐
1.1.6	(a) ¿Requieren las normas de configuración de firewalls y routers la revisión del conjunto de reglas de éstos, por lo menos, cada seis meses?	☐	☐
	(b) ¿Se revisan los conjuntos de reglas del firewall y router, por lo menos, cada seis meses?	☐	☐
1.2	¿Restringen las configuraciones para firewalls y routers las conexiones entre redes no confiables y cualquier sistema en el entorno de los datos de titulares de tarjeta de la manera siguiente? Nota: Una “red no confiable” es toda red que es externa a las redes que pertenecen a la entidad en		

evaluación y/o que excede la capacidad de control o administración de la entidad.

1.2.1	(a) ¿Está restringido el tránsito entrante y saliente a la cantidad necesaria para el entorno de los datos de titulares de tarjetas y se documentan las restricciones?	☐	☐
	(b) ¿Se niega todo el resto del tránsito entrante o saliente (por ejemplo, mediante la utilización de una declaración explícita "negar todos" o una negación implícita después de una declaración de permiso)?.	☐	☐
1.2.2	¿Están asegurados y sincronizados los archivos de configuración del router?	☐	☐
1.2.3	¿Están instalados firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y, estos firewalls están configurados para negar y controlar (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde el entorno inalámbrico hacia el entorno del titular de la tarjeta?	☐	☐
1.3	¿Prohíbe la configuración de firewall el acceso directo público entre Internet y cualquier componente del sistema en el entorno de datos de los titulares de tarjetas de la manera siguiente?		
1.3.1	¿Se implementó un DMZ para limitar el tráfico entrante sólo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado?	☐	☐

1.3.2	¿Está restringido el tránsito entrante de Internet a las direcciones IP dentro del DMZ?	☐	☐
1.3.3	¿Están permitidas las conexiones directas para el tráfico saliente o entrante entre Internet y el entorno del titular de la tarjeta?	☐	☐
1.3.4	¿Se prohibió que las direcciones internas pasen de Internet al DMZ?	☐	☐
1.3.5	¿Está el tráfico saliente desde el entorno de datos del titular de la tarjeta a Internet expresamente autorizado?	☐	☐
1.3.6	¿Está implementada la inspección completa, también conocida como filtrado dinámico de paquetes, (es decir, sólo se permiten conexiones establecidas en red)?	☐	☐
1.3.7	¿Se colocaron los componentes del sistema que almacenan datos de titulares de tarjetas (como una base de datos) en una zona de red interna, segregada desde un DMZ y otras redes no confiables?	☐	☐
1.3.8	(a) ¿Se implementaron métodos para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde en Internet? Nota: Entre los métodos para ocultar direcciones IP se pueden incluir, a modo de ejemplo: • Traducción de Dirección de Red (NAT)	☐	☐

- Ubicar servidores que contengan datos de titulares de tarjetas detrás de servidores proxy/firewalls o cachés de contenido,
- Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas,
- Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas.

(b) ¿Se autorizó la divulgación de direcciones IP privadas y de información de enrutamiento a entidades externas? ☐ ☐

1.4 (a) ¿Está instalado y activado un software de firewall personal en toda computadora móvil o de propiedad de los trabajadores con conectividad directa a Internet (por ejemplo, laptops que usan los trabajadores) mediante las cuales se accede a la red de la organización? ☐ ☐

(b) ¿Está configurado el software de firewall personal en función de normas específicas y ningún usuario de computadoras móviles y/o propiedad de los trabajadores puede alterarlo? ☐ ☐

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

Respuesta a la Pregunta de PCI DSS:	**Sí**	**No**	**Especial***
2.1 ¿Se cambian siempre los valores predeterminados por el proveedor antes de instalar un sistema en la red?	☐	☐	

Los valores predeterminados por el proveedor incluyen, a modo de ejemplo, contraseñas, cadenas comunitarias de protocolo simple de administración de red (SNMP) y la eliminación de cuentas innecesarias.

2.1.1 Para entornos con tecnología inalámbrica conectados al el entorno de datos del titular de la tarjeta o la transmisión de datos de los titulares de tarjeta, ¿se cambian los valores predeterminados de la siguiente manera:

- ¿Se cambian las claves de cifrado predeterminadas al momento de la instalación, y se cambian cada vez que una persona que tenga conocimiento de éstas cesa en sus funciones o se traslada a otro cargo en la empresa? ☐ ☐
- ¿Se cambian las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos? ☐ ☐
- ¿Se cambian las contraseñas/frases de contraseña predeterminadas en los puntos de acceso? ☐ ☐
- ¿Se actualiza el firmware de los dispositivos inalámbricos a los efectos de admitir el cifrado sólido para la autenticación y la transmisión en redes inalámbricas? ☐ ☐
- ¿Se cambian otros valores de seguridad de sistemas inalámbricos predeterminados por los proveedores, si corresponde? ☐ ☐

2.2 - ¿Se desarrollaron normas de configuración para todos los componentes del sistema, las cuales, además, se corresponden con las normas de alta seguridad aceptadas en la industria? ☐ ☐

  Entre las fuentes de normas de alta seguridad aceptadas en la industria se pueden incluir, a modo de ejemplo, SysAdmin Audit Network Security (SANS)

Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) y Center for Internet Security (CIS).

- ¿Se actualizan las normas de configuración del sistema cuando se identifican nuevo problemas de vulnerabilidad, tal como se define en el requisito 6.2? ☐ ☐

- ¿Se aplican las normas de configuración de sistemas cuando se configuran nuevos sistemas? ☐ ☐

- ¿Incluyen las normas de configuración de sistemas lo siguiente?

2.2.1 (a) ¿Se implementó una sola función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor? ☐ ☐

(Por ejemplo, los servidores web, los servidores de bases de datos y los DNS se deben implementar en servidores separados).

(b) ¿Si se utilizan tecnologías de virtualización, se implementa una sola función principal por componente de sistema o dispositivo virtual? ☐ ☐

2.2.2 (a) ¿Sólo los servicios necesarios, protocolos, daemons, etc son habilitados según lo exija la función del sistema (los servicios y protocolos que no sean directamente necesarios para desempeñar la función especificada del dispositivo están inhabilitadas)? ☐ ☐

(b) ¿Se justifican todos los servicios, daemons o protocolos habilitados no seguros, y se documentaron e implementaron funciones de seguridad? ☐ ☐

(Por ejemplo, utilice tecnologías aseguradas, tales como SSH, S-FTP, SSL o IPSec VPN, para proteger servicios no

seguros como NetBIOS, archivos compartidos, Telnet, FTP, etc.)

2.2.3 (a) ¿Tienen conocimiento los administradores del sistema y/o el personal que configura los componentes del sistema de los parámetros de configuración de seguridad comunes correspondientes a dichos componentes del sistema? ☐ ☐

(b) ¿Están incluidos los parámetros de configuración de seguridad del sistema en las normas de configuración de sistemas? ☐ ☐

(c) ¿Se configuraron apropiadamente los parámetros de seguridad en los componentes del sistema? ☐ ☐

2.2.4 (a) ¿Se eliminaron todas las funcionalidades innecesarias, tales como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios? ☐ ☐

(b) ¿Se documentaron todas las funciones habilitadas y admiten éstas una configuración segura? ☐ ☐

(ca) ¿Están presentes en los componentes del sistema sólo las funcionalidades documentadas? ☐ ☐

2.3 ¿Se cifró el acceso administrativo que no es de consola de la siguiente manera?

Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y otros tipos de acceso administrativo que no sea de consola.

(a) ¿La totalidad del acceso administrativo que no es de consola se cifra con criptografía sólida, y se invoca un método de cifrado sólido antes de que se solicite una contraseña de administrador? ☐ ☐

(b) ¿Lo servicios del sistema y archivos de parámetros son configurados de modo que impidan el uso de Telnet y otros comandos de inicio de sesión remotos inseguros? ☐ ☐

(c) ¿El acceso de administradores a la interfaz de administración basada en la web está cifrado mediante una sólida criptografía? ☐ ☐

2.4 ¿Si es un proveedor de hosting compartido, configuró los sistemas para proteger el entorno hosting y los datos de los titulares de tarjetas? ☐ ☐

Consulte el Anexo A: Requisitos adicionales de las PCI DSS para los proveedores de hosting compartido, *para enterarse de los requisitos específicos que se deben cumplir.*

PROTEGER LOS DATOS DEL TITULAR DE LA TARJETA

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.

	Respuesta a la Pregunta de PCI DSS:	**Sí**	**No**	**Especial***
3.1	¿Están implementados los procedimientos y políticas para la retención y eliminación de datos de la siguiente manera?			
3.1.1	(a) ¿Están implementados los procedimientos y las políticas de retención y eliminación de datos e incluyen requisitos específicos para la retención de datos de titulares de tarjetas tal como se requiere para fines de negocio, legales y/o regulatorios? *Por ejemplo, los datos de los titulares de tarjetas que se retendrán durante un período X por razones de negocio.*	☐	☐	

(b) ¿Incluyen las políticas y los procedimientos cláusulas para la disposición segura de los datos cuando ya no sean necesarios por razones legales, reglamentarias o de negocio, incluida la disposición de datos de titulares de tarjetas? ☐ ☐

(c) ¿Incluyen las políticas y los procedimientos la cobertura de todo almacenamiento de datos de titulares de tarjetas? ☐ ☐

(d) ¿Incluyen los procesos y procedimientos por lo menos una de las siguientes opciones? ☐ ☐

- Un proceso programático (automático o manual) para eliminar, por lo menos trimestral, datos de titulares de tarjetas almacenados que excedan los requisitos definidos en la política de retención de datos

- Requisitos para una revisión, la cual se debe realizar por lo menos trimestralmente, para verificar que los datos de titulares de tarjetas almacenados no excedan los requisitos definidos en la política de retención de datos.

(e) ¿Reúnen todos los datos de titulares de tarjetas los requisitos definidos en la política de retención de datos? ☐ ☐

3.2 (a) ¿En el caso de los emisores de tarjetas y/o las empresas que respaldan servicios de emisión y almacenan datos confidenciales de autenticación, existe una justificación de negocio para el ☐ ☐

almacenamiento de datos confidenciales de autenticación y dichos datos están asegurados?

(b) ¿Para el resto de las entidades, si se reciben y borran datos confidenciales de autenticación, se ponen en práctica procesos de eliminación de datos a fin de verificar que los datos sean irrecuperables? ☐ ☐

(c) ¿Todos los sistemas se adhieren a los siguientes requisitos de no-almacenamiento de datos de autenticación confidenciales después de la autorización (incluso si son cifrados)?

3.2.1 ¿Bajo ninguna circunstancia se almacena el contenido completo de pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo)? ☐ ☐

Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética.

Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:

- *El nombre del titular de la tarjeta.*
- *Número de cuenta principal (PAN).*
- *Fecha de vencimiento.*
- *Código de servicio*

Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.

3.2.2	¿Bajo ninguna circunstancia se almacena el código o valor de verificación de la tarjeta (número de tres o cuatro dígitos impresos en el anverso o el reverso de una tarjeta de pago)?	☐	☐
3.2.3	¿Bajo ninguna circunstancia se almacena el número de identificación personal (PIN) o el bloqueo del PIN cifrado?	☐	☐
3.3	¿Se oculta el PAN cuando aparece (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos se muestran)? *Notas:* • *Este requisito no se aplica a trabajadores y a otras partes con una necesidad de negocio legítima de conocer el PAN completo;* • *Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]).*	☐	☐
	¿Se hace el PAN ilegible en cualquier lugar donde se almacene (incluidos repositorios de datos, medios digitales portátiles, medios de copia de seguridad y registros de auditoría) utilizando cualquiera de los siguientes métodos? • Valores hash de una vía basados en cifrado sólido (el hash debe ser de todo el PAN). • Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN)	☐	☐

- Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura).
- Criptografía sólida con procesos y procedimientos asociados para la gestión de claves.

Nota: Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.

3.4.1 ¿Cuándo se utiliza el cifrado de discos (en lugar del cifrado de bases de datos a nivel de archivo o columna), se administra el acceso de la siguiente manera?

(a) ¿Se administra el acceso lógico a sistemas de archivos cifrados independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no utilizando bases de datos de cuentas de usuarios locales)? ☐ ☐

(b) ¿Se almacenan de manera segura las claves criptográficas (por ejemplo, se almacenen en medios extraíbles protegidos adecuadamente con controles sólidos de acceso)? ☐ ☐

	(c) ¿Se cifran los datos de titulares de tarjetas que se encuentran en medios extraíbles donde quiera que se almacenen? *Nota: Si no se utiliza el cifrado de disco para cifrar medios portátiles, los datos almacenados en estos medios deberán quedar ilegibles mediante algún otro método.*	☐	☐
3.5	¿Se protegen las claves utilizadas para asegurar los datos de titulares de tarjetas contra divulgación o uso indebido de la siguiente manera? *Nota: Este requisito también se aplica a las claves de cifrado de claves utilizadas para proteger las claves de cifrado de claves. Dichas claves de cifrado de claves deben ser por lo menos tan sólidas como las claves de cifrado de datos.*		
3.5.1	¿Se restringe el acceso a las claves de cifrado al número mínimo de custodios necesarios?	☐	☐
3.5.2	(a) ¿Se almacenan las claves en formato cifrado, y las claves de cifrado de claves se almacenan separadas de las claves de cifrado de datos?	☐	☐
	(b) ¿Se almacenan las claves criptográficas de forma segura en la menor cantidad de ubicaciones y formas posibles?	☐	☐
3.6	• ¿Se documentan e implementan por completo todos los procesos y procedimientos de administración de claves para las claves criptográficas utilizadas en el cifrado de los datos de titulares de tarjetas?	☐	☐

- Sólo para proveedores de servicio: ¿Si se comparten claves con clientes para la transmisión o almacenamiento de datos de titulares de tarjetas, se proporciona documentación a los clientes que incluya directrices sobre cómo transmitir, almacenar y actualizar de manera segura las claves del cliente de conformidad con los requisitos 3.6.1 a 3.6.8 que aparecen a continuación? ☐ ☐

- ¿Se implementan los procesos y procedimientos de administración de claves de modo que requieran lo siguiente?

3.6.1 ¿Incluyen los procedimientos de claves criptográficas la generación de claves criptográficas sólidas? ☐ ☐

3.6.2 ¿Incluyen los procedimientos de claves criptográficas la distribución de claves criptográficas seguras? ☐ ☐

3.6.3 ¿Incluyen los procedimientos de claves criptográficas el almacenamiento de claves criptográficas seguro? ☐ ☐

3.6.4 ¿Incluyen los procedimientos de claves criptográficas los cambios de claves criptográficas por claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que una clave dada haya producido cierta cantidad de texto cifrado), según lo define el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la ☐ ☐

industria (por ejemplo, NIST Special Publication 800-57)?

3.6.5

- ¿Incluyen los procedimientos de claves criptográficas el retiro o reemplazo (por ejemplo, mediante archivo, destrucción y/o revocación) de claves criptográficas cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro)? ☐ ☐
- ¿Incluyen los procedimientos de claves criptográficas el reemplazo de claves cuando se sepa o sospeche que están comprometidas? ☐ ☐
- ¿Si se retienen las claves criptográficas retiradas o reemplazadas, sólo se utilizan estas claves para operaciones de descifrado/verificación (no para operaciones de cifrado)? ☐ ☐

3.6.6 ¿Incluyen los procedimientos de claves criptográficas un conocimiento dividido y un control doble de claves criptográficas (por ejemplo, que requiera que dos o tres personas, que sólo tengan conocimiento de su propio componente de la clave, reconstruyan toda la clave) para las operaciones de administración de claves de cifrado en texto claro? ☐ ☐

Nota: Los ejemplos de operaciones manuales de gestión de claves incluyen, entre otros:

generación, transmisión, carga, almacenamiento y destrucción de claves.

3.6.7	¿Incluyen los procedimientos de claves criptográficas la prevención de sustitución no autorizada de claves criptográficas?	☐	☐
3.6.8	¿Se requiere que los custodios de claves criptográficas reconozcan formalmente (ya sea de manera escrita o electrónica) que entienden y aceptan sus responsabilidades como custodios de las claves?	☐	☐

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

	Respuesta a la	**Pregunta de PCI DSS:**	**Sí**	**No**	**Especial***
4.1	•	¿Se utilizan criptografía y protocolos de seguridad sólidos, como SSL/TLS o IPSEC, para salvaguardar datos confidenciales de titulares de tarjetas durante su transmisión a través de redes públicas abiertas?	☐	☐	
		Como ejemplos de redes públicas abiertas que se encuentran dentro del ámbito de aplicación de las PCI DSS se pueden mencionar, sin sentido limitativo, Internet, las tecnologías inalámbricas, el sistema global de comunicaciones móviles (GSM) y el servicio de radio por paquetes generales (GPRS).			
	•	¿Sólo se aceptan claves/certificados de confianza?	☐	☐	

- ¿Se implementan protocolos de seguridad para utilizar sólo configuraciones seguras, y no admitir versiones o configuraciones inseguras? ☐ ☐
- ¿Se implementa el nivel de cifrado adecuado para la metodología de cifrado que se utiliza (ver recomendaciones de proveedores/mejores prácticas)? ☐ ☐
- Para implementaciones de SSL/TLS: ☐ ☐

    1. ¿HTTPS aparece como parte del URL (Universal Record Locator) del navegador?

    2. ¿Los datos de los titulares de tarjeta se exigen únicamente si HTTPS aparece en la URL?

4.1.1 ¿Se aplican las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) para implementar el cifrado sólido para la autenticación y transmisión para redes inalámbricas de transmisión de datos de los titulares de tarjeta conectados con el entorno de datos del titular de la tarjeta? ☐ ☐

Nota: La utilización de WEP como control de seguridad se prohibió a partir del 30 de junio de 2010.

4.2 - ¿Se hacen ilegibles o se aseguran los números PAN con criptografía sólida siempre que se envían a través de tecnologías de mensajería de usuario final (por ejemplo, correo electrónico, mensajería instantánea o chat)? ☐ ☐

- ¿Se implementaron políticas que especifiquen que no se deben enviar números PAN sin protección a través de tecnologías de mensajería del usuario final? ☐ ☐

MANTENER UN PROGRAMA DE ADMINISTRACIÓN DE VULNERABILIDAD

Requisito 5: Utilizar y actualizar con regularidad los programas o software antivirus

	Respuesta a la Pregunta de PCI DSS:	**Sí**	**No**	**Especial***
5.1	¿Se instala software anti-virus en todos los sistemas comúnmente afectados por software malicioso?	☐	☐	
5.1.1	¿Todos los programas antivirus son capaces de detectar, eliminar y proteger contra todos los tipos conocidos de software malicioso (por ejemplo, virus, troyanos, gusanos, spyware, adware y rootkit)?	☐	☐	
1.1	¿Está actualizado todo el software anti-virus, funcionando activamente, y generando registros de auditoría, de la siguiente manera?			
	• ¿La política anti-virus requiere la actualización del software anti-virus y sus definiciones?	☐	☐	
	• ¿Está la instalación maestra del software habilitada para la actualización automática y los análisis periódicos?	☐	☐	
	• ¿Están habilitadas las actualizaciones automáticas y análisis periódicos?	☐	☐	

- ¿Están todos los mecanismos anti-virus generando registros de auditoría, y ¿son conservados los registros de conformidad con el Requisito 10.7 de las PCI DSS? ☐ ☐

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

	Respuesta a la	**Pregunta de PCI DSS:**	**Sí**	**No**	**Especial***
6.1	(a)	¿Todos los componentes de sistemas y software cuentan con los parches de seguridad más recientes proporcionados por los proveedores para protección contra vulnerabilidades conocidas?	☐	☐	
	(b)	¿Se instalan parches de seguridad crítica en un lapso de un mes contado a partir de su fecha de lanzamiento? *Nota: Las organizaciones pueden tener en cuenta la aplicación de un enfoque basado en el riesgo a los efectos de priorizar la instalación de parches. Por ejemplo, al priorizar infraestructura de importancia (por ejemplo, dispositivos y sistemas públicos, bases de datos) superiores a los dispositivos internos menos críticos a los efectos de asegurar que los dispositivos y los sistemas de alta prioridad se traten dentro del periodo de un mes y se traten dispositivos y sistemas menos críticos dentro de un periodo de tres meses.*	☐	☐	
6.2	(a)	¿Existe un proceso para identificar vulnerabilidades de seguridad recientemente descubiertas, incluida una clasificación de riesgos	☐	☐	

que se asigna a dichas vulnerabilidades? (Como mínimo, las vulnerabilidades más críticas que representen los riesgos más altos se deben clasificar como “Alto”).

Nota: Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria. Por ejemplo, los criterios para clasificar vulnerabilidades de ”Alto” riesgo pueden incluir una puntuación base CVSS de 4.0 o superior, y/o un parche proporcionado por el proveedor clasificado por el mismo como “crítico”, y/o una vulnerabilidad que afecte un componente crítico del sistema.

La clasificación de vulnerabilidades se considera una buena práctica hasta el 30 de junio de 2012, fecha a partir de la cual se convertirá en un requisito.

(b) ¿Incluyen los procesos para identificar las nuevas vulnerabilidades de seguridad el uso de fuentes externas de información sobre vulnerabilidades de seguridad? ☐ ☐

6.3

- ¿Se basan los procesos de desarrollo de software en las normas y/o mejores prácticas de la industria? ☐ ☐
- ¿Se incluye la seguridad de la información en todo el ciclo de vida de desarrollo del software? ☐ ☐
- ¿Se desarrollan aplicaciones de software de conformidad con las PCI DSS (por ejemplo, autenticación y registros seguros)? ☐ ☐

- ¿Aseguran los procesos de desarrollo de software lo siguiente?

6.3.1 ¿Se eliminan las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes de que las aplicaciones se activen o se pongan a disposición de los clientes? ☐ ☐

6.3.2 ¿Se revisan todos los cambios de código de las aplicaciones personalizadas (ya sea utilizando procesos manuales o automatizados) antes de ponerlas a disposición de la producción o los clientes a fin de identificar cualquier vulnerabilidad potencial en la codificación de la siguiente manera? ☐ ☐

- ¿Son responsables de la revisión de los cambios a los códigos individuos distintos al autor que originó el código e individuos con conocimiento de técnicas de revisión de código y prácticas de codificación segura?
- ¿Aseguran las revisiones de los códigos que éstos se desarrollan de acuerdo con las directrices de codificación segura (consulte el Requisito 6.5 de las PCI DSS)?
- ¿Se implementan las correcciones pertinentes antes del lanzamiento?
- ¿Revisa y aprueba la gerencia los resultados de la revisión de códigos antes del lanzamiento?

Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos

pueden ser realizadas por personal interno con conocimiento o terceros. Las aplicaciones web también están sujetas a controles adicionales, si son públicas, a los efectos de tratar con las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.

6.4	¿Se siguen los procesos y procedimientos de control de cambios para todos los cambios de los componentes del sistema a efectos de incluir lo siguiente?	☐	☐
6.4.1	¿Están separados los entornos de prueba/desarrollo del entorno de producción y se implementa un control del acceso para reforzar la separación?	☐	☐
6.4.2	¿Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción?	☐	☐
6.4.3	¿*No* se utilizan los datos de producción (PAN activos) para las pruebas ni para el desarrollo?	☐	☐
6.4.4	¿Se eliminan los datos de las pruebas y las cuentas antes de activar los sistemas de producción?	☐	☐
6.4.5	(a) ¿Se documentan los procedimientos de control de cambios relacionados con la implementación de los parches de seguridad y las modificaciones de software, además, requieren éstos los puntos del 6.4.5.1 al 6.4.5.4 que aparecen a continuación? (b) ¿Se realiza lo siguiente para todos los cambios?	☐	☐
6.4.5.1	¿Documentación de incidencia?	☐	☐

6.4.5.2	¿Aprobación de cambio documentada por las partes autorizadas?	☐	☐
6.4.5.3	(a) ¿Prueba de funcionalidad a fin de verificar que el cambio no incide de forma adversa en la seguridad del sistema?	☐	☐
	(b) ¿En el caso de cambios del código personalizado, se prueban las actualizaciones de conformidad con el Requisito 6.5 de las PCI DSS antes de la implementación para producción?	☐	☐
6.4.5.4	¿Se preparan los procedimientos administrativos para cada cambio?	☐	☐
6.5	• ¿Se desarrollan aplicaciones basándose en directrices de codificación segura?	☐	☐
	¿(Por ejemplo, la *Guía de proyectos de seguridad para aplicaciones web abiertas (OWASP), SANS CWE Top 25, CERT Secure Coding, etc.*)?		
	• ¿Tienen conocimiento los desarrolladores de las técnicas de codificación segura?	☐	☐
	• ¿Se cubre la prevención de vulnerabilidades comunes de codificación en el proceso de desarrollo de software a fin de asegurar que las aplicaciones no sean vulnerables a, como mínimo, lo siguiente?		
	Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.9 eran congruentes con las mejores prácticas de la industria cuando se publicó esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan, se deben		

utilizar las mejores prácticas actuales para estos requisitos.

6.5.1	¿Errores de inyección, en especial, errores de inyección SQL? (valide la entrada para verificar que los datos de usuario no pueden modificar el significado de los comandos y las consultas, utilice las consultas basadas en parámetros, etc.). *También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.*	☐	☐
6.5.2	¿Desbordamiento de buffer? (validar límites del buffer y truncar cadenas de entrada).	☐	☐
6.5.3	¿Almacenamiento criptográfico inseguro? (Prevenga errores de cifrado).	☐	☐
6.5.4	¿Comunicaciones inseguras? (Cifrar adecuadamente todas las comunicaciones autenticadas y confidenciales).	☐	☐
6.5.5	¿Manejo inadecuado de errores? (No filtre información por medio de mensajes de error).	☐	☐
6.5.6	¿Todas las vulnerabilidades "altas" detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.2 de las PCI DSS)? *Nota: Este requisito se considera una mejor práctica hasta el 30 de junio de 2012, y a partir de entonces se convierte en requisito.*	☐	☐

¿En caso de aplicaciones web e interfaces de aplicaciones (internas o externas), se tratan también las siguientes vulnerabilidades adicionales?

6.5.7 ¿Lenguaje de comandos entre distintos sitios (XSS)? (Valide todos los parámetros antes de la inclusión, utilice técnicas de escape sensibles al contexto, etc.). ☐ ☐

6.5.8 ¿Control de acceso inapropiado, tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios? (Autentique usuarios de forma correcta y desinfecte entradas. No exponga referencias a objetos internos a usuarios). ☐ ☐

6.5.9 ¿Falsificación de solicitudes entre distintos sitios (CSRF)? (No confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente). ☐ ☐

6.6 ¿En cuanto a las aplicaciones web públicas, se tratan las nuevas amenazas y vulnerabilidades de manera constante, y se las protege contra ataques conocidos aplicando *alguno* de los siguientes métodos? ☐ ☐

- Revisión de aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, de la siguiente manera:

    1. Por lo menos, anualmente
    2. Después de cualquier cambio
    3. Por una organización que se especialice en seguridad de aplicaciones
    4. Que se corrijan todas las vulnerabilidades

5. Que la aplicación se vuelva a analizar después de las correcciones

– o –

- Instalación de un firewall de aplicación web delante de aplicaciones web públicas a los efectos de detectar y de evitar ataques basados en la web.

Nota: "La organización que se especializa en seguridad de aplicación" puede ser una tercera empresa o una organización interna, siempre que los revisores se especialicen en seguridad de aplicaciones y puedan demostrar independencia respecto del equipo de desarrollo.

IMPLEMENTAR MEDIDAS SÓLIDAS DE CONTROL DE ACCESO

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

	Respuesta a la Pregunta sobre las PCI - DSS:	**Sí**	**No**	**Especial***
7.1	¿Se limita el acceso a los componentes del sistema y a los datos de titulares de tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso, de la manera siguiente?:			
7.1.1	¿Los derechos de acceso para usuarios con ID privilegiados están restringidos a los privilegios mínimos necesarios para llevar a cabo las responsabilidades del trabajo?	☐	☐	
7.1.2	¿Los privilegios se asignan a personas de acuerdo con su clasificación y función de su cargo (también	☐	☐	

	denominados "control de acceso por funciones" o RBAC).?		
7.1.3	¿Se requiere una aprobación documentada de partes autorizadas (por escrito o electrónicamente) que especifique los privilegios requeridos?	☐	☐
7.1.4	¿Se implementan controles de acceso a través de un sistema de control de acceso automatizado?	☐	☐
7.2	¿Se implementó un sistema de control de acceso para los componentes del sistema con usuarios múltiples que restrinja el acceso basado en la necesidad del usuario de conocer y que se configure para “negar todo”, salvo que se permita específicamente, de la siguiente manera?	☐	☐
7.2.1	¿Se implementaron sistemas de control de acceso en todos los componentes del sistema?	☐	☐
7.2.2	¿Están configurados los sistemas de control de acceso a los efectos de hacer cumplir los privilegios asignados a los individuos sobre la base de la clasificación de la tarea y la función?	☐	☐
7.2.3	¿Poseen los sistemas de control de acceso un ajuste predeterminado de "negar todos"? *Nota: Algunos sistemas de control de acceso se establecen de forma predeterminada para "permitir todos", y así permite acceso salvo que, o hasta que, se escriba una regla que niegue ese acceso en particular.*	☐	☐

Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora

Respuesta a la	Pregunta sobre las PCI DSS:	Sí	No	Especial*
8.1	¿Se asigna a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a los datos de titulares de tarjetas?	☐	☐	
8.2	¿Además de asignar una ID única, se emplean uno o más de los siguientes métodos para autenticar a todos los usuarios? • Algo que el usuario sepa, como una contraseña o frase de seguridad • Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente • Algo que el usuario sea, como un rasgo biométrico	☐	☐	
8.3	¿Está la autenticación de dos factores incorporada a la red de empleados, administradores y terceros para el acceso remoto (acceso en el nivel de la red desde fuera de la red) ? *(Por ejemplo, autenticación remota y servicio dial-in (RADIUS) con tokens; o sistema de control de acceso mediante control del acceso desde terminales (TACACS) con tokens;* u otras tecnologías que faciliten la autenticación de dos factores) *Nota: La autenticación de dos factores exige utilizar dos de los tres métodos de autenticación (consulte el Requisito 8.2 de las PCI DSS para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces*	☐	☐	

(por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de dos factores.

8.4	(a) Se hacen ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante un cifrado sólido?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se cifran todas las contraseñas de los clientes?	☐	☐
8.5	¿Se implementaron los controles administrativos adecuados para la autenticación e identificación de usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera?		
8.5.1	¿Se controlan la adición, eliminación y modificación de las ID de usuario, credenciales y otros objetos de identificación, tales como las ID de usuario que sólo se implementan con autorización (incluidas las que tienen privilegios específicos)?	☐	☐
8.5.2	¿Se verifica la identidad del usuario antes de restablecer contraseñas para solicitudes de usuarios realizadas a través de un método no personal (por ejemplo, teléfono, correo electrónico o web)?	☐	☐
8.5.3	¿Se configuran la primera contraseña y las contraseñas restablecidas en un valor único para cada usuario, y debe cada usuario cambiar su contraseña de inmediato después del primer uso?	☐	☐
8.5.4	¿Se desactiva o elimina de manera inmediata el acceso de cualquier usuario cesante?	☐	☐

8.5.5	¿Se eliminan o desactivan las cuentas de usuario que hayan permanecido inactivas durante más de 90 días?	☐	☐
8.5.6	(a) ¿Las cuentas utilizadas por los proveedores para el acceso remoto, mantenimiento o soporte están habilitadas sólo durante el período de tiempo necesario?	☐	☐
	(b) ¿Las cuentas de acceso remoto de los proveedores son supervisadas sólo cuando están utilizándose?	☐	☐
8.5.7	¿Se comunican los procedimientos y las políticas de autenticación a todos los usuarios que tengan acceso a los datos de titulares de tarjetas?	☐	☐
8.5.8	¿Se prohíben las cuentas y contraseñas grupales, compartidas o genéricas u otros métodos de autenticación, de la siguiente manera? Las ID de usuario y cuentas genéricas se inhabilitan o eliminan; No existen las ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas; y Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema	☐	☐
8.5.9	(a) ¿Se cambian las contraseñas de los usuarios por lo menos cada 90 días?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se requiere que las contraseñas de usuarios no consumidores se cambien periódicamente y que éstos reciban	☐	☐

	orientación sobre cuándo, y bajo cuáles circunstancias, se deben cambiar las contraseñas?		
8.5.10	(a) ¿Se requiere una contraseña de por lo menos siete caracteres de extensión?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se requiere que las contraseñas de los usuarios no consumidores cumplan con requisitos de extensión mínima?	☐	☐
8.5.11	(a) ¿Deben las contraseñas contener tanto caracteres numéricos como alfabéticos?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se requiere que las contraseñas de usuarios no consumidores contengan caracteres numéricos y alfabéticos?	☐	☐
8.5.12	(a) ¿Debe una persona enviar una contraseña nueva que sea diferente de cualquiera de las últimas cuatro contraseñas que utilizó?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se requiere que las contraseñas de usuarios no consumidores sean diferentes de las últimas cuatro contraseñas que utilizaron?	☐	☐
8.5.13	(a) ¿Están limitados los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos?	☐	☐
	(b) Sólo para proveedores de servicio: ¿Se bloquean temporalmente las contraseñas de usuarios no consumidores después de no más de seis intentos de acceso no válidos?	☐	☐
8.5.14	¿Después que se ha bloqueado una contraseña de usuario, se establece la duración del bloqueo en un	☐	☐

mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario?

8.5.15	¿Si una sesión estuvo inactiva durante más de 15 minutos, se vuelven a autenticar los usuarios (por ejemplo, al volver a escribir la contraseña) para que se active nuevamente la terminal o sesión?	☐	☐
8.5.16	(a) ¿Se autentican todos los accesos a cualquier base de datos que contenga datos de titulares de tarjetas? (Esto incluye el acceso de aplicaciones, administradores y demás usuarios).	☐	☐
	(b) ¿Realizan los usuarios las actividades relacionadas con la base de datos, tales como el acceso, las consultas y otras acciones (por ejemplo, mover, copiar, eliminar) sólo a través de métodos de programación (por ejemplo, a través de procedimientos almacenados)?	☐	☐
	(c) ¿Se limita el acceso directo o las consultas de usuarios a la base de datos a los administradores de la base de datos?	☐	☐
	(d) ¿Sólo pueden las aplicaciones (y no usuarios ni otros procesos) utilizar las ID de aplicaciones con acceso a la base de datos?	☐	☐

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta

Respuesta a la	**Pregunta sobre las PCI - DSS:**	**Sí**	**No**	**Especial***
9.1	¿Existen controles apropiados de entrada a la empresa para limitar y supervisar el acceso físico a	☐	☐	

sistemas en el entorno de datos de titulares de tarjetas?

9.1.1 • ¿Hay cámaras de video y/u otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales? ☐ ☐

Nota: "Áreas confidenciales" hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan datos de titulares de tarjetas. No se incluyen las áreas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.

- ¿Se protegen las cámaras de video y/u otros mecanismos de control de acceso contra alteraciones y desactivaciones? ☐ ☐
- ¿Se revisan y correlacionan con otras entradas los datos recogidos de cámaras de video y/u otros mecanismos de control de acceso y se almacenan los datos durante por lo menos tres meses, a menos que lo restrinja la ley? ☐ ☐

9.1.2 ¿Se encuentra restringido el acceso físico a conexiones de red de acceso público (por ejemplo, no están habilitados los puertos de red de las áreas a las que pueden acceder los visitantes, a menos que exista una autorización explícita)? ☐ ☐

¿De forma alternativa, se acompaña a los visitantes en todo momento en las áreas con conexiones de red activos?

9.1.3 ¿Se encuentra restringido el acceso físico a puntos de acceso, puertas de enlace, dispositivos portátiles, hardware de redes/comunicaciones y líneas de telecomunicaciones? ☐ ☐

9.2 ¿Se desarrollan procedimientos que permitan distinguir fácilmente entre los empleados y los visitantes, de la siguiente manera?

A los fines del Requisito 9, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, contratistas y consultores que estén físicamente presentes en las instalaciones de la entidad. "Visitante" se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones durante un tiempo no prolongado, generalmente no más de un día.

(a) ¿Incluyen los procesos y procedimientos para asignar placas de identificación a empleados y visitantes lo siguiente: ☐ ☐

- Asignación de placas de identificación,
- Cambio de requisitos de acceso y
- Revocación de placas de identificación de personal local cesante y de visitante vencidas?
- ¿Está limitado el acceso al sistema de placas de identificación al personal autorizado? ☐ ☐

(c) ¿Identifican las placas de identificación de manera clara a los visitantes y establecen una clara diferencia entre empleados y visitantes? ☐ ☐

9.3	¿Se trata a todos los visitantes de la siguiente manera?		
9.3.1	¿Se autorizan los visitantes antes de ingresar a áreas en las que se procesan o se conservan datos de titulares de tarjetas?	☐	☐
9.3.2	(a) ¿Reciben los visitantes un token físico otorgado (por ejemplo, una placa de identificación o dispositivo de acceso) que identifique a los visitantes como no empleados?	☐	☐
	(b) ¿Se vencen las placas de identificación de los visitantes?	☐	☐
9.3.3	¿Se solicita a los visitantes entregar el token físico antes de salir de las instalaciones de la empresa o al momento del vencimiento?	☐	☐
9.4	• ¿Se utiliza un registro para dar cuenta del acceso físico a las instalaciones de la empresa, así como también a las salas de informática y los centros de datos donde se guardan o se transmiten datos de titulares de tarjetas?	☐	☐
	• ¿Contiene el registro el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico y se conserva el registro del visitante durante por lo menos tres meses?	☐	☐
9.5	• ¿Se almacenan los medios de copias de seguridad en un lugar seguro, preferentemente en un lugar externo a la empresa, como un centro alternativo o para	☐	☐

	copias de seguridad, o un centro de almacenamiento comercial?		
	(b) ¿Se revisa la seguridad del lugar por lo menos una vez al año?	☐	☐
9.6	¿Todos los medios de almacenamiento cuentan con medidas de seguridad físicas (incluyendo, sin sentido limitativo, a computadoras, medios extraíbles electrónicos, recibos en papel, informes de papel y faxes)? *A los efectos del Requisito 9 "medios" se refiere a todos los medios en papel y electrónicos que contienen datos de titulares de tarjetas.*	☐	☐
9.7	• ¿Se lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios?	☐	☐
	• ¿Incluyen los controles lo siguiente:		
9.7.1	¿Están clasificados los medios de manera que se pueda determinar la confidencialidad de los datos?	☐	☐
9.7.2	¿Los medios se envían por correo seguro u otro método de envío que se pueda rastrear con precisión?	☐	☐
9.8	¿Se mantienen registros para el seguimiento de todos los medios que se trasladan desde una zona restringida, y se obtiene aprobación de la gerencia antes de trasladar los medios (especialmente cuando se distribuyen a personas)?	☐	☐
9.9	¿Se lleva un control estricto sobre el almacenamiento y accesibilidad de los medios?	☐	☐

9.9.1	¿Se mantienen adecuadamente los registros de inventario de todos los medios, además, se realizan los inventarios de medios periódicos por lo menos una vez al mes?	☐	☐
9.10	¿Se destruyen todos los medios cuando ya no son necesarios por razones comerciales o legales? La destrucción debe realizarse de la siguiente manera:	☐	☐
9.10.1	(a) ¿Se cortan en tiras, incineran o se transforman en pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas?	☐	☐
	(b) ¿Se aplican medidas de seguridad los contenedores que almacenan información que será destruida, a fin de impedir acceso al contenido? (Por ejemplo, un contenedor para corte en tiras cuenta con una traba para impedir el acceso a su contenido).	☐	☐
9.10.2	¿Se hacen irrecuperables los datos de titulares de tarjetas guardados en dispositivos electrónicos a través de un programa con la función de borrado seguro de acuerdo con las normas aceptadas en la industria para lograr una eliminación segura, o bien mediante la destrucción de los medios de forma física (por ejemplo, degaussing o destrucción magnética), de modo que los datos de los titulares de tarjetas no se puedan reconstruir?	☐	☐

SUPERVISAR Y EVALUAR LAS REDES CON REGULARIDAD

Requisito 10: Rastrear y supervisar todos los accesos a los recursos de Red y datos de los titulares de las tarjetas.

Respuesta a la	Pregunta sobre las PCI DSS:	Sí	No	Especial*
10.1	¿Existe algún proceso para vincular todos los accesos a componentes del sistema (especialmente el acceso con privilegios administrativos, tales como los de raíz) a cada usuario en particular?	☐	☐	
10.2	¿Se implementan pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?			
10.2.1	Todos los usuarios acceden a los datos de titulares de tarjetas.	☐	☐	
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos.	☐	☐	
10.2.3	Acceso a todas las pistas de auditoría.	☐	☐	
10.2.4	Intentos de acceso lógico no válidos.	☐	☐	
10.2 5	Uso de mecanismos de identificación y autenticación.	☐	☐	
10.2.6	Inicialización de los registros de auditoría.	☐	☐	
10.2.7	Creación y eliminación de objetos en el nivel del sistema.	☐	☐	
10.3	¿Se registran las siguientes entradas de pistas de auditoría de todos los componentes del sistema para cada evento?			
10.3.1	Identificación de usuarios.	☐	☐	
10.3.2	Tipo de evento.	☐	☐	

10.3.3	Fecha y hora.	☐	☐
10.3.4	Indicación de éxito o fallo.	☐	☐
10.3.5	Origen del evento.	☐	☐
10.3.6	Identidad o nombre de los datos, componentes del sistema o recurso afectados.	☐	☐
10.4	(a) ¿Se sincronizan todos los relojes y horas críticos del sistema a través del uso de la tecnología de sincronización de hora, la cual se mantiene actualizada? *Nota: Un ejemplo de tecnología de sincronización es el Network Time Protocol (NTP).* (b) ¿Se implementan los siguientes controles para adquirir, distribuir y almacenar hora?	☐	☐
10.4.1	(a) ¿Sólo reciben los servidores de hora centrales designados señales de fuentes externas y poseen todos los sistemas críticos la misma hora correcta, según la Hora Atómica Universal o UTC?	☐	☐
	(b) ¿Interactúan entre sí los servidores de hora centrales designados para mantener una hora exacta y reciben otros servidores internos reciben señales de hora sólo de los servidores de hora centrales?	☐	☐
10.4.2	¿Se protegen los datos de tiempo de la siguiente manera: (a) ¿Se restringe el acceso a los datos de tiempo sólo a personal con una necesidad de negocio de acceder a dichos datos?	☐	☐
	(b) ¿Se registran, supervisan y revisan los cambios a los sistemas críticos?	☐	☐

10.4.3	¿Se recibe la configuración de hora de fuentes aceptadas por la industria? (Esto es para impedir que un individuo malintencionado cambie el reloj). De forma opcional, se pueden cifrar estas actualizaciones con una clave simétrica, y se pueden crear listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de tiempo (para evitar el uso no autorizado de servidores de hora internos).	☐	☐
10.5	¿Se aseguran de la siguiente manera las pistas de auditoría de manera que no se puedan alterar?		
10.5.1	¿Se limita la visualización de pistas de auditoría a quienes lo necesitan por motivos de trabajo?	☐	☐
10.5.2	¿Están protegidos los archivos de las pistas de auditoría contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes?	☐	☐
10.5.3	¿Se realizan de inmediato copias de seguridad de los archivos de las pistas de auditoría en un servidor de registros central o medios que resulten difíciles de modificar?	☐	☐
10.5.4	¿Se descargan o se copian los registros para tecnologías que interactúan con la parte externa (por ejemplo, inalámbricas, firewalls, DNS, correo) en un servidor de registros central o medios internos?	☐	☐
10.5.5	¿Se utiliza el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se	☐	☐

generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta)?

10.6 ¿Se revisan todos los componentes del sistema por lo menos una vez al día, y se exigen seguimientos a las excepciones? ☐ ☐

Las revisiones de registros deben incluir a los servidores que realizan funciones de seguridad, tales como sistema de detección de intrusiones (IDS) y servidores de protocolos de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS).

Nota: Las herramientas de recolección, análisis y alerta de registros pueden ser utilizadas para lograr cumplir con el Requisito 10.6

10.7 (a) ¿Se han implementado políticas y procedimientos de retención de registros de auditoría y éstos requieren que el historial de pistas de auditoría por al menos un año? ☐ ☐

(b) ¿Se encuentran disponibles los registros de auditoría durante al menos un año y se han implementado los procesos para restaurar de inmediato al menos los registros de los últimos tres meses para el análisis? ☐ ☐

Requisito 11: Probar periódicamente los sistemas y procesos de seguridad

Respuesta a la	**Pregunta sobre las PCI DSS:**	**Sí**	**No**	**Especial***

11.1 (a) ¿Se documenta con frecuencia trimestral el proceso implementado para detectar e identificar puntos de acceso inalámbricos? ☐ ☐

Nota: Los métodos que se pueden utilizar en el proceso incluyen, pero no se limitan a, barridos de redes inalámbricas, inspecciones físicas/lógicas de componentes del sistema e infraestructura, control de acceso a la red (NAC) o IDS/IPS inalámbrico.

Independientemente de los métodos que se utilicen, éstos deben ser suficientes para detectar e identificar cualquier dispositivo no autorizado.

(b) ¿La metodología es capaz de detectar e identificar cualquier punto de acceso, incluyendo por lo menos lo siguiente? ☐ ☐

- Tarjetas WLAN insertadas en los componentes del sistema;
- Dispositivos inalámbricos conectados a componentes del sistema (por ejemplo, por USB, etc.);
- Dispositivos inalámbricos conectados a un puerto de red o a un dispositivo de red?

(c) ¿Se realiza por lo menos trimestralmente el proceso documentado para identificar los puntos de acceso inalámbricos no autorizados sea realizado para todos los componentes e instalaciones de sistemas. ☐ ☐

(d) Si se utiliza supervisión automatizada (por ejemplo, IDS/IPS inalámbrico, NAC, etc.), ¿se ☐ ☐

	configura la supervisión para que genere alertas al personal?		
	(e) ¿El Plan de respuesta a incidentes (Requisito 12.9) incluye una respuesta en caso de que se detecten dispositivos inalámbricos no autorizados?	☐	☐
11.2	¿Se realizan escaneos internos y externos de vulnerabilidades en la red al menos trimestralmente, y después de cada cambio significativo en la red (tales como instalaciones de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos) de la manera siguiente? *Nota: No se requiere que se completen cuatro escaneos trimestrales aprobados para el cumplimiento inicial de PCI DSS si el asesor verifica que 1) el resultado del último escaneo fue un análisis aprobado, 2) la entidad ha documentado políticas y procedimientos que exigen escaneos trimestrales y 3) las vulnerabilidades detectadas en los resultados del escaneo se han corregido tal como se muestra en el nuevo escaneo. Durante los años posteriores a la revisión inicial de las PCI DSS, se deben haber realizado análisis trimestrales aprobados.*	☐	☐
11.2.1	(a) ¿Se realizan escaneos internos trimestrales de vulnerabilidades?	☐	☐
	(b) ¿El proceso de análisis interno incluye nuevos escaneos hasta que se obtienen resultados aprobados, o hasta que se resuelven todas las vulnerabilidades	☐	☐

	"Altas", de conformidad con lo definido en el Requisito 6.2 de las PCI DSS?		
	(c) ¿Los escaneos trimestrales son realizados por recurso(s) internos calificados o por terceros calificados y, si corresponde, la empresa que realiza las pruebas garantiza la independencia? (no es necesario que sea un QSA o ASV).	☐	☐
11.2.2	(a) ¿Se realizan escaneos externos trimestrales de vulnerabilidades?	☐	☐
	(b) ¿Los resultados de cada escaneo trimestral satisfacen los requisitos de la Guía del programa ASV? (por ejemplo, ausencia de vulnerabilidades con calificación mayor que 4.0 por la CVSS y ausencia de fallas automáticas).	☐	☐
	(c) ¿Los escaneos trimestrales de vulnerabilidades externas son realizados por Proveedores aprobados de escaneos (ASV), aprobados por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC)?	☐	☐
11.2.3	(a) ¿Se realizan escaneos internos y externos de las vulnerabilidades en la red después de cada cambio significativo en la red (tales como instalaciones de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos) de la manera siguiente?: *Nota: Los análisis realizados después de cambios en la red puede realizarlos el personal interno.*	☐	☐

(b) ¿El proceso de escaneo incluye nuevos análisis hasta que: ☐ ☐

- Para análisis externos, no se hayan registrado vulnerabilidades con puntuaciones mayores que 4.0, según la CVSS.
- Para escaneos internos, se haya obtenido un resultado de aprobación o todas las vulnerabilidades “Alta”, como las define el Requisito 6.2 de las PCI DSS, hayan sido resueltas.

(c) ¿Los escaneos son realizados por recurso(s) internos calificados o por terceros calificados y, si corresponde, la empresa que realiza las pruebas garantiza la independencia? (no es necesario que sea un QSA o ASV). ☐ ☐

11.3
- ¿Se realizan pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno). ☐ ☐
- ¿Se han corregido las vulnerabilidades detectadas y se han repetido las pruebas? ☐ ☐
- ¿Los escaneos son realizados por un recurso interno calificado o por un tercero calificado y, si corresponde, la empresa que realiza las pruebas garantiza la independencia? (no es necesario que sea un QSA o ASV). ☐ ☐

¿Incluyen estas pruebas de penetración lo siguiente?

11.3.1	¿Pruebas de penetración de la capa de red? *Nota: Las pruebas deben incluir a los componentes que admiten las funciones de red, así como también a los sistemas operativos.*	☐	☐
11.3.2	¿Pruebas de penetración de la capa de aplicación? *Nota: Las pruebas deben incluir, por lo menos, las vulnerabilidades que contiene el Requisito 6.5.*	☐	☐
11.4	• ¿Se utilizan sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el entorno de datos de titulares de tarjetas, así como puntos críticos dentro del entorno?	☐	☐
	• ¿Se ha configurado el IDS y/o IPS para alertar al personal ante la sospecha de riesgos?	☐	☐
	• ¿Se han actualizados todos los motores de detección y prevención de intrusiones, bases y firmas?	☐	☐
11.5	• ¿Se han implementado herramientas de supervisión de integridad de archivos dentro del entorno de datos de titulares de tarjetas? Los ejemplos de archivos que se deben supervisar incluyen: Ejecutables del sistema Ejecutables de aplicaciones Archivos de configuración y parámetros	☐	☐

Archivos de almacenamiento central, históricos o archivados, de registro y auditoría

- ¿Están configuradas las herramientas para alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de configuración o archivos de contenido, y dichas herramientas realizan comparaciones de archivos críticos al menos semanalmente? ☐ ☐

Nota: a los fines de la supervisión de integridad de archivos, los archivos críticos generalmente son los que no se modifican con regularidad, pero cuya modificación podría indicar un riesgo o peligro para el sistema. Los productos para la supervisión de integridad de archivos generalmente vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.

MANTENER UNA POLÍTICA DE SEGURIDAD DE INFORMACIÓN

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

Respuesta a la	Pregunta sobre las PCI DSS:	Sí	No	Especial*
12.1	¿Existe una política de seguridad establecida, publicada, mantenida y distribuida a todo el personal relevante?	☐	☐	

A los fines del Requisito 12, "personal" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la entidad o que tengan acceso al entorno de datos de los titulares de tarjetas en la empresa.

12.1.1	¿Aborda la política todos los requisitos de las PCI DSS?	☐	☐
12.1.2	¿Se documenta un proceso anual de evaluación de riesgos que identifique las amenazas y vulnerabilidades y que produzca como resultado una evaluación formal de riesgos? (Ejemplos de metodologías de evaluación de riesgos incluyen, pero no están limitados a: OCTAVE, ISO 27005 y NIST SP 800-30.)	☐	☐
	(b) ¿Se realiza el proceso de evaluación de riesgos por lo menos una vez al año?	☐	☐
12.1.3	¿Se revisa la política de seguridad de la información al menos una vez al año y se actualiza según sea necesario de manera que refleje los cambios en los objetivos de la empresa o el entorno de riesgos?	☐	☐
12.2	¿Se desarrollan procedimientos diarios de seguridad operativa coherentes con los requisitos de esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas de usuarios y procedimientos de revisión de registros) e incluyen procedimientos	☐	☐

	administrativos y técnicos para cada uno de los requisitos?		
12.3	¿Se desarrollan políticas de utilización para tecnologías críticas (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, tabletas, asistentes digitales/para datos personales [PDA], utilización del correo electrónico e Internet) para definir el uso adecuado de dichas tecnologías por parte de todo el personal que requieran los siguientes?	☐	☐
12.3.1	¿Aprobación explícita de las partes autorizadas para utilizar las tecnologías?	☐	☐
12.3.2	¿Autenticación para el uso de la tecnología?	☐	☐
12.3.3	¿Una lista de todos los dispositivos y el personal que tenga acceso?	☐	☐
12.3.4	¿Etiquetado de dispositivos para determinar propietario, información de contacto y objetivo?	☐	☐
12.3.5	¿Usos aceptables de la tecnología?	☐	☐
12.3.6	¿Ubicaciones aceptables para las tecnologías en la red?	☐	☐
12.3.7	¿Lista de productos aprobados por la empresa?	☐	☐
12.3.8	¿Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad?	☐	☐

12.3.9	¿Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso?	☐	☐
12.3.10	Para que el personal tenga acceso a datos de titulares de tarjetas mediante tecnologías de acceso remoto, ¿prohíbe a política copiar, mover y almacenar los datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad de negocios definida?	☐	☐
	Para el personal con la autorización correcta, ¿la política de requiere que los datos de los titulares de tarjetas sean protegidos, de acuerdo con los Requisitos de las PCI DSS?	☐	☐
12.4	¿Las políticas y los procedimientos de seguridad definen claramente las responsabilidades de seguridad de la información de todo el personal?	☐	☐
12.5	¿Se asigna formalmente la seguridad de la información a un Jefe de seguridad u otro miembro de la gerencia relacionado con la seguridad?	☐	☐
	¿Las siguientes responsabilidades de administración de seguridad de la información están asignadas a una persona o equipo?		
12.5.1	¿Se establecen, documentan y distribuyen políticas y procedimientos de seguridad?	☐	☐

12.5.2	¿Se supervisan y analizan las alertas e información de seguridad, y se distribuyen entre el personal correspondiente?	☐	☐
12.5.3	¿Establecimiento, documentación y distribución de los procedimientos de respuesta ante incidentes de seguridad y escala para garantizar un manejo oportuno y efectivo de todas las situaciones?	☐	☐
12.5.4	¿Administración de las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones?	☐	☐
12.5.5	¿Supervisión y control todo acceso a datos?	☐	☐
12.6	(a) ¿Se ha implementado un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos de los titulares de tarjetas? (b) ¿Incluyen los procedimientos de los programas de concienciación sobre seguridad lo siguiente?	☐	☐
12.6.1	¿El programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los empleados en lo relativo a la concienciación (por ejemplo, carteles, cartas, notas, capacitación basada en web, reuniones y promociones)? *Nota: Los métodos pueden variar según el rol del personal y su nivel de acceso a los datos de titulares de tarjetas.*	☐	☐

	¿Se educa al personal inmediatamente después de la contratación y por lo menos una vez al año?	☐	☐
12.6.2	¿Se exige al personal que reconozca al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa?	☐	☐
12.7	¿Se verifican los antecedentes del personal potencial (consulte la definición de "personal" en el Requisito 12.1, arriba) antes de la contratación a fin de minimizar el riesgo de ataques de fuentes internas? (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias). *Nota: En el caso del personal potencial que se va a contratar como cajeros de un comercio, que sólo tienen acceso a un número de tarjeta a la vez al realizarse una transacción, este requisito constituye sólo una recomendación.*	☐	☐
12.8	Si los datos de titulares de tarjeta se comparten con proveedores de servicios, ¿se mantienen e implementan políticas y procedimientos para administrarlos y controlarlos de la siguiente manera?		
12.8.1	¿Se mantiene una lista de proveedores de servicios?	☐	☐
12.8.2	¿Se mantiene un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de	☐	☐

	los datos de titulares de tarjetas que ellos tienen en su poder?		
12.8.3	¿Existe un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso?	☐	☐
12.8.4	¿Se mantiene un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios con una frecuencia anual, como mínimo?	☐	☐
12.9	¿Se ha implementado un plan de respuesta a incidentes como preparación para reaccionar inmediatamente a un fallo del sistema, de la siguiente manera?		
12.9.1	• ¿Se ha creado un plan de respuesta a incidentes para implementarlo en caso de fallos en el sistema?	☐	☐
	• ¿El plan trata lo siguiente cómo mínimo?		
	• ¿Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago?	☐	☐
	• ¿Procedimientos específicos de respuesta a incidentes?	☐	☐
	• ¿Procedimientos de recuperación y continuidad comercial?	☐	☐

- ¿Procesos de realización de copia de seguridad de datos? ☐ ☐
- ¿Análisis de los requisitos legales para el informe de riesgos? ☐ ☐
- ¿Cobertura y respuestas de todos los componentes críticos del sistema? ☐ ☐
- ¿Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago? ☐ ☐

12.9.2 ¿Se realiza una prueba del plan al menos una vez al año? ☐ ☐

12.9.3 ¿Se ha designado personal especializado que se encuentre disponible permanentemente para responder a las alertas? ☐ ☐

12.9.4 ¿Se proporciona capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad? ☐ ☐

12.9.5 ¿Se incluyen alertas de sistemas de detección y prevención de intrusiones, y de monitorización de integridad de archivos en el plan de respuesta a incidentes? ☐ ☐

12.9.6 ¿Se ha elaborado un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria? ☐ ☐