ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ESQUEMA IDEAL BÁSICO DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA MEDIANA PROVEEDORA DE SERVICIOS"

EXÁMEN DE GRADO (COMPLEXIVO)

Previa la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

PATRICIA ISABEL PENAFIEL BARRERA

GUAYAQUIL-ECUADOR

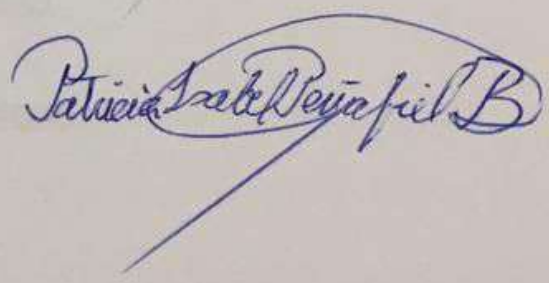
AÑO: 2016

AGRADECIMIENTO

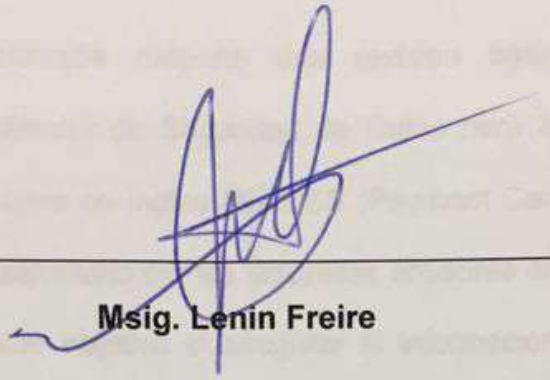
En primer lugar quiero agradecer a Dios, que cada día nos da la oportunidad de ser la mejor versión de quien somos y por permitirme culminar esta etapa en mi carrera, a mi esposo e hija por amarme apoyarme y darme ánimo, a mis padres por todo el esfuerzo por darme siempre lo mejor, a la Lic. Pilar Giler por todas recomendaciones en la Maestría y al Mg. Armando Altamirano por aconsejarme al inicio de mi carrera estudiantil en la ESPOL y a todos esos profesores profesionales de esta institución, en especial a Mg. Karina Astudillo y Mg. Albert Espinal.

DEDICATORIA

Dedico este trabajo a Mi Roca y Refugio, quien conforta mi alma y en quien confío Dios, a mis padres y abuela Floricelda Bernal (+) porque ningún esfuerzo será suficiente para honrarlos y mi hija –mi princesa- que este fruto sea inspiración para ti.

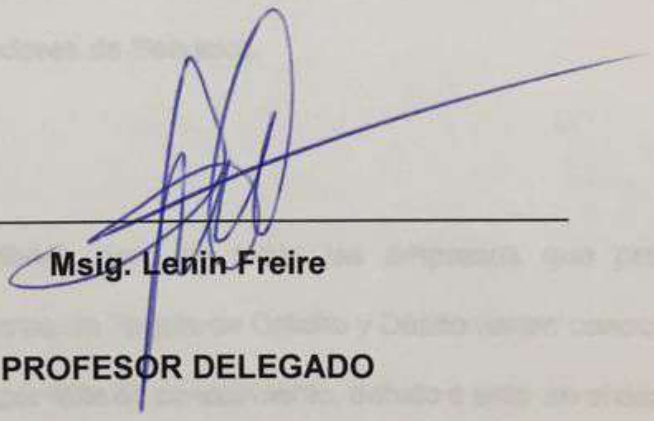


TRIBUNAL DE SUSTENTACIÓN



Msig. Lenin Freire

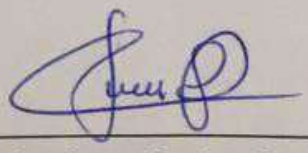
DIRECTOR MSIA



Msig. Lenin Freire

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Msig. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El Proyecto a continuación propone una revisión básica o guía para implementación del estándar de Seguridad de Datos para la industria de las tarjetas de pago sus siglas en Ingles PCI-DSS (Payment Card Industry – Data Security Standard), desarrollado por las empresas emisoras de tarjeta de Débito y Crédito, y tiene como objetivo el asegurar la información relacionada con tarjetas de crédito y débito, la cual es exigida actualmente a las Instituciones Financieras en Ecuador por la Superintendencia de Bancos, pero no sólo está relacionada con las Instituciones Financieras, sino también a empresas comerciales y para proveedores de Servicios.

Esta Norma es Internacional, pero no todas las empresas que procesan, almacenan o transmiten Datos de Tarjeta de Crédito y Débito tienen conocimiento o se apegan a ella, quizás por falta de conocimiento, debido a esto en el desarrollo de este documento revisaremos el Marco Referencial, conceptos básicos, su aplicabilidad y revisión de los 12 dominios de la Normativa PCI – DSS con la finalidad de indicar productos principales o medidas básicas, que nos ayuden a solventar lo requerido para el cumplimiento básico de la misma y mejorar la seguridad institucional.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CAV: Valor de autentificación de la tarjeta de pago JCB.

CID: Número de Identificación de la tarjeta de pago American Express y Discover.

CVC: Código de Validación de la Tarjeta de pago MasterCard.

CVV: Valor de Verificación de la Tarjeta para tarjetas de pago Visa y Discover.

DMZ: Zona Desmilitarizada.

ISO: Organización Internacional de Normalización.

IPS: Sistema de Protección de Intrusiones..

MAC: Control de Accesos a Medios.

PAN: Número de Cuenta Principal.

PCI-DSS: Estándar de Seguridad de Datos.

PCI SCC: Consejo Nacional de Normas de Seguridad de Industrias de Tarjetas de Pago.

PIN: Número de Identificación Personal.

QSA: Auditores de Seguridad Calificados.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Este documento pretende ser una guía para implementación de un modelo de Seguridad de la Información, basada en la Norma Internacional para la Industria de Tarjetas de Pago todas las empresas que procesen, almacenen o transmitan datos de Tarjetas y deberían apegarse a esta norma.

En el Capítulo I, se expondrá la descripción del problema, los objetivos generales. En el Capítulo II, se establecerá el Marco Teórico que describirá la estructura o elementos de los datos de los titulares de Tarjetas, su aplicabilidad, exclusiones y restricciones. En el Capítulo III, se revisarán los 12 dominios abordando las recomendaciones o productos que nos pueden ayudar para la implementación de la Noma PCI DSS.

CAPÍTULO 1

GENERALIDADES

El Consejo Nacional de Nomas de Seguridad de Industrias de Tarjetas de Pago (PCI-SCC), en el año 2006 y con la finalidad de establecer un estándar y reducir los riesgos por el uso de Tarjeta de crédito, como resultado la creación a tres tipos de estándares, y estos estándares son [4]:

1. **PCI-DSS.-** Destinado a Instituciones Financieras, empresas de servicios en los que procesen, almacenen o transmiten datos de Tarjetas de Crédito.

2. **PA-DSS.-** Para Empresas que vendan aplicaciones que procesen datos de Tarjeta de Pago.

3. **PCI-PTS.-** Para Entidades que desarrollen dispositivos con PIN y quienes utilicen estos.

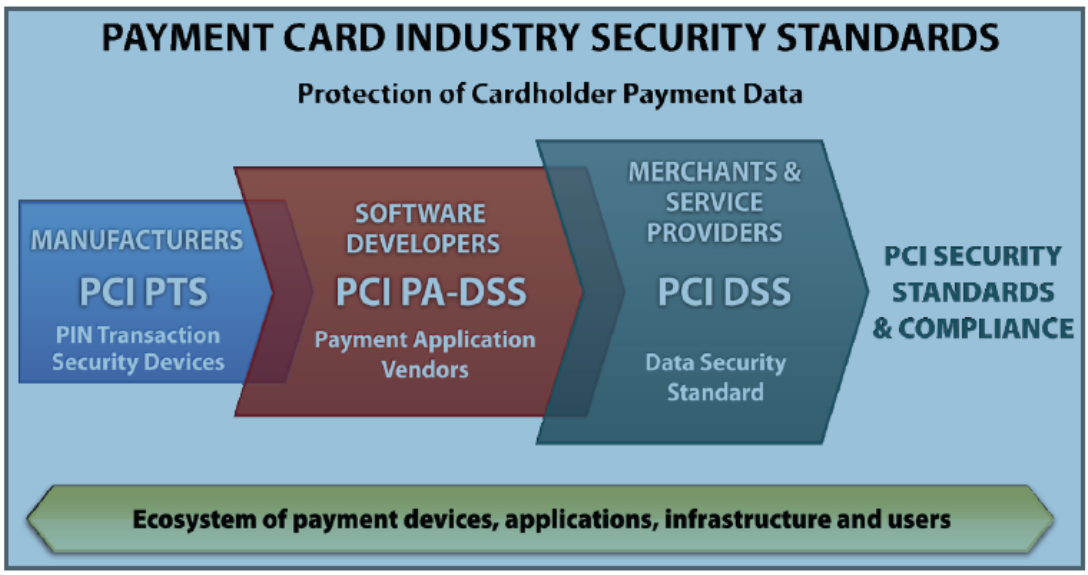


Figura 1.1: Estándares definidos por la PCI-SCC [1].

Fuente: PCI-DSS.

Para este trabajo de tesis la Norma que revisaremos será PCI-DSS.

1.1 DESCRIPCIÓN DEL PROBLEMA

En Ecuador la Superintendencia de Bancos mediante la Resolución “JB-2012-2148” [2] se basa en esta norma, y afecta directamente a las entidades Financieras, puntualmente a Bancos y Seguros con el objetivo de establecer un Sistema de Procesamiento Seguro para la Información del tarjetahabiente. Pero no solo las Entidades Financieras transaccionan o comercializan mediante el uso de Tarjetas de Crédito/Débito y estas también pueden tener proveedores de

servicios o socios estratégicos que estén relacionados al tratamiento de información de Tarjetahabiente y mayor aun la mayoría de las empresas que pertenecen al sector de Comercial desconoce esta norma y lo crítico es que por falta de conocimiento al realizar transacciones se almacene no sólo cédula y nombre del titular de la tarjeta, sino también el PAN, la fecha de expiración y código de verificación, que sea Hackeada y toda esa información se utilice para robar la identidad del titular de la tarjeta para realizar consumos no autorizados. Pero como saber qué requisitos se deben cumplir de esta Norma y que productos me pueden ayudar con el cumplimiento de la misma?

1.2 OBJETIVOS GENERALES

Realizar una guía que provea información básica de esta norma, recomendaciones y productos que nos pueden ayudar a la alineación a esta Norma Internacional, y reducir el riesgo ataques Informáticos que conllevaría a reclamos por Fraudes, multas por incumplimientos y para mejorar competitivamente en base al respaldo que obtenemos al estar alineados con PCI-DSS .

CAPÍTULO 2

MARCO REFERENCIAL

La Norma PCI-DSS es un estándar de Seguridad que establece un conjunto de requisitos, mediante la utilización de políticas y procedimientos de seguridad y diseño de software con la finalidad buscar proteger los datos del titular de la tarjeta y datos de autentificación confidenciales y disminuir el riesgo de fraude por mal uso de estos, mediante los siguientes requisitos [5]:

Tabla 1: Requerimientos PCI-DSS.

Construir y mantener una red segura.	Instale y mantenga una configuración de Firewall para proteger los datos del Titular de la Tarjeta.
	No utilizar las contraseñas de Sistemas y otros parámetros de seguridad provistos por los proveedores.

Proteja los datos del Titular de la Tarjeta.	Proteja los datos de usuarios de tarjetas almacenados.
	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un Programa de Administración de Vulnerabilidades.	Proteger todos los sistemas contra malware y actualizar loa programas o Antivirus regularmente.
	Desarrollar Sistemas y Aplicaciones Seguras
Implementar Medidas de Control de Acceso.	Restrinja el Acceso a los Datos del titular de la tarjeta según la necesidad de de saber del negocio.
	Identificar y autentificar el acceso a los componentes del Sistema.
	Restringir el acceso físico a los datos del titular de la tarjeta.

Supervisar y Evaluar las redes con regularidad.	Pruebe con regularidad los sistemas y procesos de Seguridad.
	Mantenga una política que aborde la seguridad de la Información

Fuente: PCI-DSS.

2.1 ELEMENTOS DE DATOS DE LOS TITULARES DE TARJETAS

Las tarjetas de pago contienen los Datos del titular de la Tarjeta y los datos confidenciales de autentificación.

Tabla 2: Elementos de una Tarjeta de Pago.

Datos Tarjetahabientes	Datos Confidenciales de Autentificación
PAN o Número de Cuenta Principal.	Información Almacenada en la Pista magnética o en su Chip. No se puede almacenar según requisito 3.2
Nombres del Titular.	Números CAV2 (JBC)/CVC2 (MasterCard)/ CVV2 (Visa)/CID (American Express) usados como Códigos de Validación. No se puede almacenar según requisito 3.2

Fecha de Expiración.	Pin/Bloqueo de PIN (Número de Identificación Personal). No se puede almacenar según requisito 3.2
Código de Servicio.	

Fuente: PCI-DSS [3].

Ubicados de cómo se puede observar en la figura a continuación.

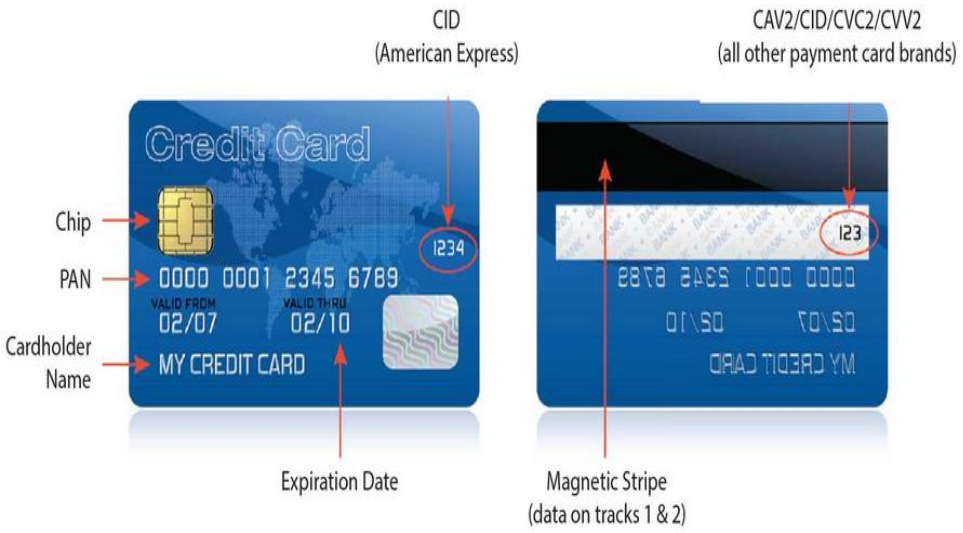


Figura 2.1: Ubicación de Datos Titular de Tarjetas.

Fuente: PCI-DSS.

2.2 APLICABILIDAD

Las compañías que procesan, almacenan o transmiten datos de tarjetas deben cumplir con este estándar pero según la cantidad de transacciones con Tarjetas de Crédito y según ente emisor de Tarjeta varía el peso para

evaluar de cumplimiento.

COMERCIOS				
Nivel	**Criterio Visa**	**Criterio Mastercard**	**Req de Validación**	**Validado**
1	Cualquier comercio que procesa > 6.000.000 de transacciones por año independientemente del canal. Cualquier comercio que haya sufrido un ataque donde los datos hayan quedado comprometidos. Cualquier comercio que Visa o Mastercard considere. Cualquier comercio clasificado de nivel 1 por otra marca.		Auditoría anual de seguridad anual *on-site* Escaneos trimestrales de vulnerabilidades	QSA (*Qualified Security Assessor*) o Auditor interno ASV (*Approved Scanning Vendor*)
2	Cualquier comercio ***e-commerce*** que procesa de 150.000 a 6.000.000 de transacciones por año.	Cualquier comercio ***e-commerce*** que procesa de 1.000.000 a 6.000.000 de transacciones por año. Cualquier comercio clasificado de nivel 2 por otra marca.	Cuestionario anual de autoevaluación Escaneos trimestrales de vulnerabilidades	Comercio ASV (*Approved Scanning Vendor*)
3	Cualquier comercio ***e-commerce*** que procesa de 20.000 a 150.000 transacciones por año.	Cualquier comercio ***e-commerce*** que procesa de 20.000 a 1.000.000 de transacciones por año. Cualquier comercio clasificado de nivel 3 por otra marca.		
4	El resto de comercios independientemente del canal.	El resto de comercios independientemente del canal.	Recomendado: Cuestionario anual de autoevaluación Escaneos trimestrales de vulnerabilidades	Comercio ASV (*Approved Scanning Vendor*)

Figura 2.2: Clasificación y Requerimientos de Validación para comercios.

Fuente: Isec Auditors[4]

PROVEEDORES DE SERVICIO				
Nivel	**Criterio VISA**	**Criterio Mastercard**	**Req de Validación**	**Validado**
1	Todos los procesadores VisaNet, pasarelas de pago y proveedores IPS (*Internet Payment Service*) independientemente del volumen de transacciones	Todos los TPP (*Third party processors*), DSE (*Data Storage Entity*) que almacenan datos de comercios de nivel 1 y 2	Auditoría anual de seguridad anual *on-site* Escaneos trimestrales de vulnerabilidades	QSA ASV
2	No están en el nivel 1 y almacena, transmite o procesa más de 1.000.000 al año	Todos los DSE que almacenan datos de comercios de nivel 3		
3	No están en el nivel 1 y almacena, transmite o procesa menos de 1.000.000 al año	Todos los DSE no incluidos en niveles 1 y 2	Cuestionario anual de autoevaluación Escaneos trimestrales de vulnerabilidades	Proveedor de Servicios ASV

Figura 2.3: Clasificación y Requerimientos de Validación para proveedores de servicio [4].

Fuente: Isec Auditors

2.3 EXCLUSIONES Y RESTRICCIONES

Las compañías que no procesan, almacenan o transmiten datos de tarjetas no deben cumplir con este estándar si se requiere aplicar un estándar para

seguridad de la Información podría optarse por ISO27001 o si el PAN no se almacena, procesada o transmitida tampoco se aplica.

De ser lo contrario se evaluaría la cantidad de transacciones por año para ver si aplican las auditorias o autoevaluación. Las auditorias indicadas son realizadas por Auditores autorizados (Certificados en la Norma QSAs). Los escaneos de vulnerabilidades se realizaran en todos los caso por un Proveedores Autorizado ASV.

Las compañías que si procesan, almacenan o transmiten datos de tarjetas y no se apegan al cumplimiento pueden hasta llegar a perder la franquicia de las tarjetas con las que transaccionan.

CAPÍTULO 3

SOLUCIÓN PROPUESTA

Para empresas medianas Proveedora de Servicios, si no pasan de las 20.000 transacciones por año y si no son procesadores de Visa Net, ni pasarelas de pago o proveedores de Pago por Intenet sólo deberán llenar el formulario de autoevaluación y realizar escaneos trimestrales de vulnerabilidades.

3.1 REVISIÓN Y RECOMENDACIONES PARA LOS DOMINIOS DE PCI- DSS

Para determinar el alcance e identificar como fluyen los datos de titulares de tarjeta así como en qué procesos son utilizados y además documentarlos. También es recomendable que elimine los datos de flujo de no ser necesarios, así también realizar una segmentación de red para

proteger la red de los datos de tarjetas y mantenerla aislada. Comience dimensionando la cantidad de transacciones y todos los accesos que tenga que dar, asígnelos de la forma parametrizada y como un firewall, primero está todo cerrado y se comienzan a dar los accesos.

Revise el anexo de Tareas recurrentes [6] de haber alguna auditoria serán unas de las primeras actividades que se revisaran.

3.1.1 INSTALE Y MANTENGA UNA CONFIGURACIÓN DE FIREWALL PARA PROTEGER LOS DATOS DEL TITULAR DE LA TARJETA

En este requerimiento abordamos el uso de un Firewall, el cual debe tener un procedimiento formal de cambios, constar con un diagrama de red actualizado y documentado, así también las conexiones y la administración de Firewall incluyendo las redes Wireless, y así también en los protocolos y puertos lo que no sea necesario depure, segmente y configure DMZs y restringa el tráfico hacia la información del tarjetahabiente, mantenga los archivos de configuración del Router y Firewall en un lugar seguro, retire los accesos públicos a internet dentro de la organización, implemente medidas anti-suplantación y filtrado dinámico de paquetes (implementar solución de Firewall de última generación).

3.1.2 NO UTILIZAR CONTRASEÑAS DE SISTEMAS Y OTROS PARÁMETROS DE SEGURIDAD PROVISTOS POR LOS PROVEEDORES

Cambie todo valor predeterminados por el proveedor de cualquier aplicativo o producto incluyendo el cifrado, revise frecuentemente las cuentas cambie las contraseñas y elimine las que no son necesarias, se trabajará solo los servicios necesarios, implementar funciones de seguridad para archivos compartidos, realice el inventario de componentes.

3.1.3 PROTEJA LOS DATOS DEL TITULAR DE LA TARJETA QUE FUERON ALMACENADOS

Implemente políticas y procedimientos para la eliminación de datos, estableciendo periodo de almacenamiento de datos, procedimiento formal para la eliminación segura de los datos, establezca procesos trimestrales para identificación y eliminación de datos de titulares de tarjetas, los sistemas no deben registrar datos de autentificación después de la aprobación ni cifrados, convierta al PAN en ilegible en cualquier lugar que se almacene, utilice cifrado, utilice claves para evitar la divulgación del titular, realice procedimiento de las claves criptográficas, se recomienda un Firewall de Base de Datos.

3.1.4 CIFRAR LA TRANSMISIÓN DE LOS DATOS DEL TITULAR DE TARJETA EN LAS REDES PÚBLICAS ABIERTAS

Utilice criptografía y protocolos seguros para la transmisión de los datos del titular de la tarjeta en redes públicas abiertas, se recomienda producto CERTES para cifrado de canales por hardware y realice políticas y procedimientos operativos.

3.1.5 PROTEGER TODOS LOS SISTEMAS CONTRA MALWARE Y ACTUALIZAR LOS PROGRAMAS O SOFTWARE ANTIVIRUS REGULARMENTE

Se recomienda la implementación de un Endpoint protection por ser más completos, mantenerlo actualizado, generando logs y con procedimientos de administración.

3.1.6 DESARROLLE Y MANTENGA SISTEMAS Y APLICACIONES SEGURAS

Las aplicaciones deben tener los parches actualizados, usar fuentes conocidas, clasificarla por riesgos, eliminar cuentas de desarrollo de prueba, establezca procedimiento de cambios en el código y para corregir vulnerabilidades, se establece un esquema de pruebas para los nuevos desarrollos, no utilice el PAN en pruebas o de ejemplos en las capacitaciones, separe las funciones del personal, elimine los datos de prueba, desarrolle aplicaciones seguras.

3.1.7 RESTRINJA EL ACCESO A LOS DATOS DEL TITULAR DE LA TARJETA SEGÚN LA NECESIDAD DE SABER DEL NEGOCIO.

Realice política y procedimientos de control de accesos que indique necesidades de acceso asignación de privilegios por función, cada usuario con identificador e implementar sistemas de control de acceso.

3.1.8 IDENTIFICAR Y AUTENTIFICAR EL ACCESO A LOS COMPONENTES DEL SISTEMAS.

Asignar un identificador único para cada persona y con validación de intentos fallidos en ingreso de contraseña y el mismo que le permita acceso a los sistemas y a los datos sin existir duplicidad, auditar la asignación del ID, implemente un sistema de políticas y procedimientos para los sistemas administrativos de control de usuario, controle la creación, modificación o eliminación de los usuarios, bloqueo temporales de usuario por intentos fallidos y cambio de contraseña por lo menos cada 90 días, cree políticas y procedimientos operativos.

3.1.9 RESTRINGIR EL ACCESO FÍSICO A LOS DATOS DEL TITULAR DE LA TARJETA.

Establezca policitas y procedimientos que restrinjan el acceso físico al entorno de los datos de tarjeta y establezca política de destrucción de medios, coloque cámaras en el entorno y almacene por lo menos por 90 días, de a los visitantes algún distintivo especial para identificarlos y entregarla al salir, establecer un libro de visitas, se restringen los medios

de almacenamiento y realizar inventarios habitualmente, capacitar al personal para detectar comportamiento sospechoso o indicios de alteración o sustitución de dispositivos.

3.1.10 RASTREE Y SUPERVISE TODOS LOS ACCESOS A LOS RECURSOS DE LA RED Y LOS DATOS DE LOS TITULARES DE TARJETAS.

Mantenga las pilas de auditoria habilitadas, registros de inicializaciones o pausa de los registros de auditorías con la siguiente información Identificación del usuario, tipo de Evento, Fecha y Hora, indicador de éxito, origen de evento, identidad o nombre de los datos de los componentes o recursos afectados, sincronice los procesos, realizar copias de seguridad de los archivos y pistas de auditoria, realice políticas y procedimientos para revisar una vez al día, se recomienda una herramienta NAC.

3.1.11 PRUEBE CON REGULARIDAD LOS SISTEMAS Y PROCESOS DE SEGURIDAD

Procedimientos implementados para identificar trimestralmente los puntos de accesos, escanear trimestralmente de vulnerabilidades mediante análisis internos y externos, configure herramientas para alertar de modificaciones no autorizadas, se recomienda el uso de un SIEM.

3.1.12 MANTENGA UNA POLÍTICA QUE ABORDE LA SEGURIDAD DE LA INFORMACIÓN PARA TODO EL PERSONAL

Realice una política de seguridad publicada y actualizada por lo menos 1 vez al año y divulgada a todo el personal y proceso de evaluación de riesgos anual, Listas de dispositivos junto con el personal al que se ha asignado, desconexión automática de sesiones, restringa al personal que tenga acceso a los datos de titular de la tarjeta la opción de copiar, pegar, mover. La política debe actualizarse como mínimo una vez al año y contemplar se recomienda como mínimo el desarrollo de los siguientes:

- Requerimiento de seguridad para cada una de las Aplicaciones Comerciales.
- Políticas de Divulgación y Autorización de la Información.
- Perfiles de Usuario Estándar para cada puestos de Trabajo y Horarios.
- Establecer reglas con la premisa de que todo. Qué debe estar generalmente prohibido a menos de que se dé la autorización expresa?
- Políticas y Procedimientos de Administración de Accesos de Usuario y Administración de Privilegios.
- Políticas de Control de Accesos a la Red.
- Políticas y Procedimiento de Control de Acceso al Data Center.

- Políticas y Procedimiento Asignación de Recursos Informático para el Personal.
- Establezca un Sistema de Configuración de Contraseñas.
- Inactivaciones por tiempo muerto.
- Establezca Sistema de Accesos y Uso de los Sistemas y Registro de Eventos.
- Procedimientos y Áreas de Riesgo, Registro y revisión de eventos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

Todo cambio conlleva un porcentaje de resistencia y normalmente las instituciones tampoco pueden realizar cambios debido a los costos altos para realizar las implementaciones, por el tiempo en que tomará el cambio o por la dependencia entre los servicios versus la tecnología utilizada.

1. Pero si piensa en las multas o el daño irreparable de imagen creo que reduce el precio para esta inversión.

Recomendaciones:

1. A pesar poder a llegar a tener incumplimientos se puede realizar controles para compensar los incumplimientos encontrados, si se cuenta con un argumento justificando y que describa esta limitante la cual tendrá que ser revisada por un

QSA de acuerdo lo descrito en anexo B y anexo C dentro del estándar para lo cual se tendrá que hacer uso de un control compensatorio.

A continuación algunos controles compensatorios más comunes que se pueden usar [6]

- Uso de DLP.
- Uso de control de Acceso a la red.
- Controles de ejecución mediante el uso de listas blancas.
- Control de Acceso y filtrado MAC.
- Uso de controles de filtrado de URL.

2. Procure que antes de lanzar cualquier proceso evalúe la necesidad de la información y de ser de temas comerciales, evite transmitir, almacenar o procesar datos de Tarjeta de Crédito, utilice algún otro medio de verificación y bajo ninguna circunstancia almacene datos de la banda lectora.

BIBLIOGRAFÍA

[1] PCI Council, De un vistazo Normas Panoramas
https://www.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf
fecha de consulta Diciembre 2015

[2] Superintendencia de Bancos de Ecuador- Junta Bancaria del Ecuador, Resolución "JB-2012-2148
http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf, fecha de consulta Noviembre 2015

[3] PCI Council, para revisión de los elementos de datos de los titulares de la tarjeta
https://www.pcisecuritystandards.org/documents/pci_dss_emv-es.pdf, fecha de consulta Noviembre 2015

[4] Iseca Auditores Requerimientos a Cumplir
http://www.isecauditors.com/sites/default/files/files/SIC-76_PCI-DSS_Como_cumplir.pdf
Fecha de Consulta Junio2015

[5] Noma PCI – DSS
https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Fecha de Consulta Diciembre 2015

[6] Lista de Tareas Recurrentes

http://www.pcihispano.com

Fecha de Consulta Diciembre 2015

ANEXOS

Tareas Recurrentes [4]

Req. PCI DSS v3.1	Descripción	Periodicidad
1.1.2	Actualización del diagrama de red	Cada cambio significativo
1.1.3	Actualización del diagrama de flujo de datos de tarjetas	Cada cambio significativo
1.1.7	Revisión de reglas de firewalls y routers	Semestral
1.5	Validación de aplicación de políticas de seguridad y procedimientos operativos para la gestión de firewalls	Continuamente
2.1	Cambio de valores predeterminados en sistemas	Antes de ingresar a la red
2.1.1	Cambio de valores predeterminados en equipos inalámbricos	Antes de ingresar a la red
2.2.b	Actualización de los estándares de configuración	Cuando son identificadas nuevas vulnerabilidades
2.2.3.b	Implementación de características adicionales de seguridad para cada servicio, protocolo y daemon considerado inseguro (solo para terminales POS POI)	**Después de junio 30 de 2016:** Monitorización continua de nuevas vulnerabilidades en SSL y versiones anteriores de TLS.
2.2.3.c	Implementación de características adicionales de seguridad para cada servicio, protocolo y daemon considerado inseguro (para los demás dispositivos)	**Hasta junio 30 2016:** Mantener un plan de mitigación de riesgos y migración de SSL y versiones anteriores de TLS. **Después de junio 30 de 2016:** Retiro de SSL y versiones anteriores de TLS.
2.3.e	Encriptar todo el acceso administrativo que no sea realizado por consola usando criptografía fuerte (solo para terminales POS POI)	**Después de junio 30 de 2016:** Monitorización continua de nuevas vulnerabilidades en SSL y versiones anteriores de TLS.
2.3.f	Encriptar todo el acceso administrativo que no sea realizado por consola usando criptografía fuerte (para los demás dispositivos)	**Hasta junio 30 2016:** Mantener un plan de mitigación de riesgos y migración de SSL y versiones anteriores de TLS. **Después de junio 30 de 2016:** Retiro de SSL y versiones anteriores de TLS.
2.4.a	Actualización del inventario de componentes del sistema del entorno PCI DSS	Cada cambio del entorno
2.5	Validación de aplicación de políticas de seguridad y procedimientos operativos para la gestión de cambios en valores por defecto y otros parámetros de seguridad	Continuamente
3.1.a	Proceso para eliminar datos de tarjeta almacenados fuera del umbral de retención	Trimestral
3.6.4.a	Cambio de claves de cifrado	Criptoperiodo
3.6.5.a	Retiro o remplazo de claves de cifrado	A la salida de un empleado que conozca la clave o cuando se sospeche que la clave está en riesgo

3.6.8.a	Verificación que los custodios de claves han reconocido formalmente que entienden y aceptan sus responsabilidades	Cada vez que haya un cambio de custodio
3.7	Validación de aplicación de políticas de seguridad y procedimientos operativos para la protección de datos de tarjeta almacenados	Continuamente
4.1.h	Utilice criptografía fuerte y protocolos de seguridad para proteger los datos confidenciales de tarjeta de pago durante la transmisión a través de redes públicas abiertas (solo para terminales POS POI)	**Después de junio 30 de 2016:** Monitorización continua de nuevas vulnerabilidades en SSL y versiones anteriores de TLS.
4.1.i	Utilice criptografía fuerte y protocolos de seguridad para proteger los datos confidenciales de tarjeta de pago durante la transmisión a través de redes públicas abiertas (para los demás dispositivos)	**Hasta junio 30 2016:** Mantener un plan de mitigación de riesgos y migración de SSL y versiones anteriores de TLS. **Después de junio 30 de 2016:** Retiro de SSL y versiones anteriores de TLS.
4.3	Validación de aplicación de políticas de seguridad y procedimientos operativos para la encriptación de transmisiones de datos de tarjeta	Continuamente
5.1.2	Identificación y evaluación de amenazas de malware en sistemas no afectados comúnmente por software malicioso para confirmar si necesitan o no software anti-virus	Periódicamente (La periodicidad debe ser definida por la organización)
5.2.a	Actualización de antivirus y definiciones	Continuamente
5.2.b	Ejecución de escaneos anti-virus y actualizaciones automáticas	Periódicamente (La periodicidad debe ser definida por la organización)
5.4	Validación de aplicación de políticas de seguridad y procedimientos operativos para la protección de sistemas contra malware	Continuamente
6.2	Instalación de actualizaciones de seguridad	**PCI DSS v2.0:** Mensual: Dispositivos críticos Trimestral: Dispositivos no críticos **PCI DSS v3.0 y 3.1:** Mensual: Actualizaciones críticas Otras actualizaciones: 2-3 meses (por ejemplo)
6.1	Identificación y catálogo de nuevas vulnerabilidades	Continuamente
6.3.1	Eliminación de cuentas, ID de usuario y contraseñas en aplicaciones desarrolladas	Antes de ingreso a producción
6.3.2	Revisión de código personalizado	Antes de ingreso a producción
6.4.4	Eliminación de datos y cuentas de prueba	Antes de ingreso a producción
6.5.a	Formación en técnicas de codificación segura para desarrolladores	Periódicamente (La periodicidad debe ser definida por la organización)

6.7	Validación de aplicación de políticas de seguridad y procedimientos operativos para el desarrollo y mantenimiento de sistemas seguros y aplicaciones	Continuamente
7.3	Validación de aplicación de políticas de seguridad y procedimientos operativos para la restricción de acceso a datos de tarjeta	Continuamente
8.1.3	Cancelación del acceso para cualquier usuario cesante	Inmediato
8.1.4	Eliminación/inhabilitar lcuentas de usuario inactivas	Trimestral
8.1.5	Habilitación de cuentas de acceso remoto a proveedores	Durante el periodo necesario
8.2.4	Cambio de contraseñas	Trimestral
8.1.7	Desbloqueo de cuentas de usuario por el administrador (si no se desbloquea automáticamente)	Cada vez que se bloquee la cuenta
8.8	Validación de aplicación de políticas de seguridad y procedimientos operativos para la identificación y autenticación	Continuamente
9.1.1.c	Almacenamiento de registros de acceso físico	Trimestral o conforme con la legislación vigente
9.4.4.c	Almacenamiento del registro de visitas	Trimestral o conforme con la legislación vigente
9.5.1.b	Revisión de las ubicaciones de almacenamiento de medios de copias de seguridad	Anual
9.7.1	Inventario de medios	Anual
9.8	Destrucción de medios que contengan datos de tarjetas	Cuando ya no sean necesarios
9.9.1	Actualización de la lista de dispositivos que capturan datos de tarjeta mediante interacción física directa	Periódicamente (La periodicidad debe ser definida por la organización). Puede ser ejecutado de forma manual o automática
9.9.2	Inspección de las superficies de dispositivos que capturan datos de tarjeta mediante interacción física directa en búsqueda de manipulación o sustitución	Periódicamente (La periodicidad debe ser definida por la organización)
9.9.3	Formación a personal para reportar cualquier manipulación o sustitución de dispositivos que capturan datos de tarjeta mediante interacción física directa	Periódicamente (La periodicidad debe ser definida por la organización)
9.10	Validación de aplicación de políticas de seguridad y procedimientos operativos para la restricción de acceso físico a datos de tarjetas de pago	Continuamente
10.5.3	Realización de copias de seguridad de pistas de auditoría en un servidor central	Inmediato

10.6.1	Revisión de los registros de auditoría (logs)	**PCI DSS v2.0:** Diario **PCI DSS v3.0 y 3.1:** Diario de los siguientes elementos: - Todos los eventos de seguridad - Logs de todos los componentes de sistemas que almacenan, procesan y/o transmiten datos de tarjeta y/o datos sensibles de autenticación (SAD) o que puedan impactar la seguridad de dichos datos - Logs de todos los componentes de sistema críticos - Logos de todos los servidores y componentes de sistemas que ejecuten funciones de seguridad
10.6.2	Revisión de los registros de auditoría (logs) de otros componentes del sistema	Con base en la política de la organización y estrategia de gestión de riesgos
10.7	Conservación del historial de pistas de auditoría	Trimestral (disponible) Anual
10.8	Validación de aplicación de políticas de seguridad y procedimientos operativos para la monitorización de todos los accesos a recursos de red y datos de tarjeta de pago	Continuamente
11.2.3	Realización de análisis de vulnerabilidades interno y externo	Cada cambio significativo
	Pruebas de penetración externas e internas a nivel de capa de red y capa de aplicación	Anual Cada cambio significativo
11.3.1	Pruebas de penetración externas	Anual Cada cambio significativo
11.3.2	Pruebas de penetración internas	Anual Cada cambio significativo
11.3.4	Ejecución de pruebas de penetración en el caso que se use segmentación para aislar el CDE de otras redes	Anual Cada cambio significativo
11.4.c	Actualización de IDS/IPS (motores, líneas base y firmas)	Continuamente
11.5.b	Comparación de archivos críticos (FIM)	Semanalmente
11.6	Validación de aplicación de políticas de seguridad y procedimientos operativos para la monitorización de seguridad y pruebas	Continuamente
12.2	Ejecución de un proceso que identifique las amenazas, vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Anual
12.1.1	Revisión de la política de seguridad de la información	Anual Cada cambio significativo
	Ejecución de los procedimientos de seguridad operativa	Diario
12.3.9	Activación de tecnologías de acceso remoto para proveedores y socios de negocio	Cuando sea requerido

12.6.1.b	Formación en seguridad al personal	En el momento de la contratación Anualmente
12.6.2	Reconocimiento por parte del personal de la lectura y entendimiento de la Política de Seguridad y procedimientos	Anualmente (manual o electrónico)
12.8.1	Lista de proveedores de servicio	Periódicamente (No se indica periodicidad específica)
12.8.4	Supervisión del estado de cumplimiento de PCI DSS por parte de los proveedores de servicios	Permanente
12.10.2	Prueba del plan de Respuesta a Incidentes	Anualmente
12.10.4	Formación adecuada al personal en responsabilidades de respuesta ante fallos de seguridad	Periódicamente (No se indica periodicidad específica)

Fuente Pcihispano

Productos que pueden ayudar a Implementar los requerimientos PCI-DSS

REQUERIMIENTO PCI	CONSULTORIA	FABRICANTES			
1. Instalar y mantener una configuración de Firewall para proteger la información confidencial de los usuarios.	Consultoría e Ingeniería para desarrollo en mejores prácticas de implementación de reglas en sistemas de seguridad perimetral FW	ArcSight (Reglas, Consolas y reportes) "1.1.6,1.1.7,1.1.8,1.1.9 ,1.2, 1.3.1,1.3.2, 1.3.5,1.3.6,1.3.8,1.4.1, 1.4.2"	CheckPoint (FW) "1", o servicio de Soporte Gold Plus para monitoreo de reglas y control de cambios		
2. No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores	Consultoría asesoramiento en implementación de mejores prácticas de seguridad.	ArcSight (Reglas, Consolas y reportes) "2.1,2.2.1,2.2.2"	CyberArk, Gestión de los usuarios privilegiados o de contraseñas a los sistemas sensibles con workflow de autorización		
3. Proteger los datos de usuarios de tarjetas almacenados por la compañía.	Imperva Protección de Bases de Datos.	ArcSight (Reglas, Consolas y reportes) "3.3"	McAfee DLP y Cifrado (Cifrado de Discos y de Información y prevención de perdida de información)	PGP, Cifrado de archivos y de transmisión de archivos Secure File.	

4. Cifrar los datos de usuarios de tarjetas y la información confidencial transmitida a través de redes públicas abiertas o desprotegidas	SecureFile, PGP y McAfee, soluciones para cifrado de archivos y carpetas	ArcSight (Reglas, Consolas y reportes) "4.1"	McAfee o servicio de Cifrado de Correo.	CERTES Solución para cifrado de canales por Hardware.	Active Base y Camouflaje, Solución para enmascaramiento de datos.
5. Usar y tener actualizado el software antivirus.	Escaneo de Vulnerabilidades McAfee, Vulnerability Manager	SIEM McAfee (Reglas, Consolas y reportes) "5.1,5.2"			
6. Desarrollar y mantener sistemas y aplicaciones seguras	Firewall de aplicaciones Web WAF Imperva y ASM F5	ArcSight (Reglas, Consolas y reportes) "6.4,6.5"	F5 Full aplication proxie	EasySolutions Revisión de Código	
7. Restringir y controlar el acceso a la información confidencial teniendo en cuenta las necesidades de acceso por parte de empleados a	Consultoría Clasificación de Información y Mapas de riesgos	SIEM McAfee (Reglas, Consolas y reportes) "7.1"	McAfee DLP, ForeScout NAC	F5 VPN SSL	EasySolutions, Sistema de autenticación, actúa como un segundo factor de autenticación pero más importante permite tener

la información.					registro de ingresos a sistemas evitando el no repudio
8. Asignar una identificación única a cada persona que tenga acceso a un ordenador de la compañía.	Consultoría, programas de concientización en seguridad de la información.	SIEM McAfee (Reglas, Consolas y reportes) "8.5.1,8.5.13,8.5.16,8.5.4,8.5.5,8.5.9"	EasySolutions, Sistema de autenticación, actúa como un segundo factor de autenticación pero más importante permite tener registro de ingresos a sistemas evitando el no repudio	McAfee NAC, por medio de mecanismos de autenticación de los sistemas a través de un NAC se puede saber quién esta autenticado en la red y a donde se le puede dar o no acceso.	
9. Restringir el acceso físico a los datos de los usuarios de tarjetas almacenados	Consultoría desarrollo de políticas y mejores prácticas en seguridad de la información	SIEM McAfee (Reglas, Consolas y reportes) "9.3.3"	Active Base y Camouflage para enmascaramiento de datos.	EasySolutions, Sistema de autenticación, actúa como un segundo factor de autenticación pero más importante permite tener registro de ingresos a sistemas	

				evitando el no repudio	
10. Rastrear y monitorear todo el acceso a los recursos de la red y a los datos de los usuarios de tarjeta.	SIEM McAfee (Reglas, Consolas y reportes) "10.2.1,10.2.2,10.2.4,10.2.5,10.2.6,10.2.7,10.3,10.4,10.5.210.5.5"	EasySolutions, Sistema de autenticación, actual como un segundo factor de autenticación pero más importante permite tener registro de ingresos a sistemas evitando el no repudio	McAfee NAC, por medio de mecanismos de autenticación de los sistemas a través de un NAC se puede saber quién esta autenticado en la red y a donde se le puede dar o no acceso.		
11. Probar regularmente los sistemas y los procesos de seguridad	Consultoría pruebas de penetración y Ethical Hacking	SIEM McAfee (Reglas, Consolas y reportes) "11.1,11.2"	McAfee Vulnerability Manager e ISS Enterprise Scanner		

12. Mantener una política que contemple la Seguridad de la Información	Consultoría diseño de Red ideal segura y mejores prácticas en seguridad de la información, implementación de defensa en profundidad.	SIEM McAfee (Consolas y reportes) "12.1.2,12.3.7,12.8,12.9,12.9.5,12.9.6"	AllGress permite tener un dashboard de validación de cumplimiento de políticas de seguridad basado en un framework de seguridad que puede integrar diferentes estándares como PCI, ISO 2700x entre otros.		

Fuente: NetSecure-Proveedor de Soluciones