

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**



**Facultad de Ingeniería en Electricidad y Computación**

**Maestría en Seguridad Informática Aplicada**

**“ELABORACIÓN DEL HARDENING (ASEGURAMIENTO) DE  
UNA BASE DE DATOS SQL SERVER DE UNA EMPRESA  
PROCESADORA DE TARJETAS DE CRÉDITO”**

**EXAMEN DE GRADO (COMPLEXIVO)**

Previa a la obtención del grado de:

**MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

LINA ROSA ORELLANA ÁLVAREZ

Guayaquil – Ecuador

AÑO: 2015

## **AGRADECIMIENTO**

Agradezco infinitamente a Dios, por las bendiciones recibidas cada día, por ser mi refugio en todo momento, por ser el camino que me da seguridad, por ser mi guía que llena de luz divina mi vida. A mis padres y a mi familia, por brindarme su apoyo, su esfuerzo, por confiar en mí y apoyar mis decisiones, gracias por hacerme sentir que soy valiosa, comparto este logro con ustedes. A mis amigos y amigas, por esas palabras sinceras en los momentos oportunos, por tener la voluntad de ayudar, sin importar la distancia ni el tiempo. A mis compañeros de aula y de trabajo, por su compañerismo, por su compromiso y empeño, pues juntos nos llevamos la satisfacción del deber cumplido en los diferentes desafíos que tuvimos que enfrentar, espero tener la dicha de trabajar juntos de nuevo en una nueva oportunidad. A mis profesores, por brindarme su paciencia, su apoyo, sus observaciones, sus comentarios, gracias por haber compartido sus conocimientos y experiencias. A todas las personas, que directa o indirectamente me han ayudado en mi formación como ser humano y profesional.

## DEDICATORIA

Dedico este trabajo a Dios, por ser esa Fuerza Divina que me protege y sostiene. A mis padres y a mi familia, por creer en mí, pues es lo que necesito para hacer realidad mis sueños y triunfar. A mis amigos, por alentarme con sus palabras para seguir hasta cumplir mis metas, por dedicar su tiempo, los momentos vividos los recordaré con cariño. A mis compañeros de aula y de trabajo y profesores, por creer que con el trabajo cooperativo se alcanzan resultados de calidad, gracias por ayudarme a mejorar y adquirir más experiencia en el camino como una profesional. A todas las personas que creen que las ideas irreales, con perseverancia, pueden ser reales.

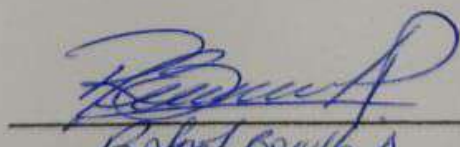
## TRIBUNAL DE SUSTENTACIÓN



Mg. Laura Ureta

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Mg. Albert Espinal

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

## RESUMEN

Este documento presenta la metodología usada para la elaboración del procedimiento del Aseguramiento "*Hardening*" de una base de datos en SQL Server de una empresa procesadora de tarjetas de crédito para cumplimiento del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

Para lo cual se consideró los siguientes aspectos:

- Configuración de la Base de Datos
- Control de Acceso
- Políticas de Contraseñas
- Auditoría

## ÍNDICE GENERAL

AGRADECIMIENTO .....	ii
DEDICATORIA .....	iii
TRIBUNAL DE SUSTENTACIÓN .....	iv
RESUMEN .....	v
ÍNDICE GENERAL.....	vi
ABREVIATURAS Y SIMBOLOGÍAS .....	viii
ÍNDICE DE FIGURAS.....	x
ÍNDICE DE TABLAS .....	xi
INTRODUCCIÓN .....	xii
CAPÍTULO 1 .....	1
GENERALIDADES .....	1
1.1. REGULACIONES PCI .....	1
1.2. ENTIDADES QUE DEBEN CUMPLIR CON PCI-DSS.....	3
1.2.1. COMERCIOS .....	3
1.2.2. PROVEEDORES DE SERVICIO.....	4
1.3. APLICABILIDAD DE LAS PCI-DSS SOBRE LOS ELEMENTOS DE LOS DATOS DEL TITULAR DE LA TARJETA.....	5
1.4. REQUISITOS DE LA NORMA PCI-DSS .....	7
1.5. ASEGURAR UNA BASE DE DATOS COMO PARTE DEL CUMPLIMIENTO DE LA NORMA PCI .....	9
CAPÍTULO 2.....	11

METODOLOGÍA USADA .....	11
2.1. FASE I: ANÁLISIS PRELIMINAR.....	11
2.2. FASE II: PLAN DE ACCIÓN .....	15
2.2.1. REQUISITO 2 DE LA NORMA PCI.....	15
2.2.2. REQUISITO 3 DE LA NORMA PCI.....	15
2.2.3. REQUISITO 4 DE LA NORMA PCI.....	17
2.2.4. REQUISITO 6 DE LA NORMA PCI.....	18
2.2.5. REQUISITO 7 DE LA NORMA PCI.....	19
2.2.6. REQUISITO 8 DE LA NORMA PCI.....	20
2.2.7. REQUISITO 10 DE LA NORMA PCI.....	21
CAPÍTULO 3.....	25
ANÁLISIS DE RESULTADOS.....	25
3.1. HERRAMIENTAS .....	25
3.2. REPORTES PARA AUDITORÍAS .....	27
CONCLUSIONES Y RECOMENDACIONES .....	30
BIBLIOGRAFÍA.....	34

## ABREVIATURAS Y SIMBOLOGÍAS

<b>Hardening</b>	Conjunto de actividades con la finalidad de reforzar la seguridad en un componente.
<b>PAN</b>	Es el número de cuenta principal de una tarjeta bancaria.
<b>PCI-DSS</b>	Sus siglas en inglés corresponden a Payment Card Industry Data Security Standard, en español significa Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
<b>PCI-SSC</b>	Sus siglas en inglés corresponden a Payment Card Industry Security Standard Council, en español significa Consejo de Normas de Seguridad de las Industrias de Tarjetas de Pago.
<b>SSL</b>	Sus siglas en inglés corresponden a Secure Sockets Layer, en español significa Capa de Conexión Segura.



**Tarjetahabiente** Persona que es dueña de una tarjeta de crédito.

**TDE** Sus siglas en inglés corresponden a Transparent Data Encryption, en español significa Cifrado de datos transparente.

**VPN** Sus siglas en inglés corresponden a Virtual Private Network, en español significa Red Virtual Privada.

## ÍNDICE DE FIGURAS

Figura 1.1. Niveles de cumplimiento de comercios. [6].....	4
Figura 1.2. Niveles de cumplimiento de proveedores de servicio. [6] .....	4
Figura 1.3. Procedimientos de cumplimiento PCI-DSS. [6].....	5
Figura 1.4. Datos de cuentas. [2].....	6
Figura 1.5. Ubicación de datos de una tarjeta de crédito. [5].....	6
Figura 1.6. Norma de seguridad de datos de la PCI. [2].....	7
Figura 1.7. Ciclo de Deming orientado al cumplimiento de PCI-DSS. [4].....	9

## ÍNDICE DE TABLAS

Tabla 1. Normas de Seguridad PCI-DSS, PA-DSS y PCI-PTS. [1] .....	2
Tabla 2. Tabla de Usuarios Inactivos con Cuentas Activas .....	27
Tabla 3. Tabla de Usuarios que tienen Privilegios Administrativos .....	28
Tabla 4. Tabla de Logins Recientes de Administrador .....	28
Tabla 5. Tabla de Recientes Operaciones Privilegiadas .....	29

## INTRODUCCIÓN

Las entidades procesadoras de tarjetas de crédito deben cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) con el fin de evitar fraudes durante el procesamiento, almacenamiento o transmisión de datos confidenciales relacionados a la tarjeta.

Para esto, se debe llevar a cabo medidas de seguridad para todos los componentes del sistema que conforman dicho proceso, uno de los equipos, es el servidor de base de datos, específicamente el motor de base de datos, ya que es el lugar donde reposa la información de los datos de los tarjetahabientes, por lo que se debe evitar que la información sea interceptada o modificada.

En el presente documento expondré medidas de seguridad para minimizar las amenazas en un motor de base de datos SQL Server con el fin de cumplir los requerimientos que exige el PCI, así como también algunas consideraciones adicionales que se deben tener en cuenta mientras se realiza este proceso.

# **CAPÍTULO 1**

## **GENERALIDADES**

### **1.1. REGULACIONES PCI**

En el año 2006, se reunieron cinco prestigiosas marcas de tarjetas de crédito, conformaron el Consejo de Normas de Seguridad de las Industrias de Tarjetas de Pago (PCI SSC) y crearon tres diferentes estándares con la finalidad de mitigar los riesgos de estafas que pudieran darse con los datos de las tarjetas bancarias. [1]

Estos estándares se aplican a tres tipos de entidades diferentes dependiendo de cómo interactúe con la tarjeta, los cuales especifico en la Tabla 1, la entidad se encuentra en la obligatoriedad de cumplir con la norma correspondiente.

El presente documento se va a enfocar en una empresa procesadora de tarjetas de crédito, por lo que sólo se tratará de la norma PCI-DSS.

Tabla 1. Normas de Seguridad PCI-DSS, PA-DSS y PCI-PTS. [1]

<b>Norma</b>	<b>Dirigido a:</b>
PCI-DSS	Entidades bancarias, comerciantes y entidades que brindan servicios en los que se procesa, almacena y/o transmite datos de tarjetas de pago.
PA-DSS	Entidades que venden y desarrollan aplicaciones con las que procesan datos de tarjetas de pago.
PCI PTS	Entidades que desarrollan dispositivos y realizan transacciones con PIN, define los requisitos que deben cumplir en cuanto al diseño, fabricación y transporte de dichos dispositivos, así como las entidades que los utilicen.

## **1.2. ENTIDADES QUE DEBEN CUMPLIR CON PCI-DSS**

Todas las empresas que operen con información sobre titulares de tarjetas – sin tomar en cuenta el tamaño – tienen que demostrar el cumplimiento con el DSS. [6]

Es aplicable en todos los negocios donde la información de tarjeta-habientes sea:

- Procesada
- Almacenada
- Transmitida

Estas empresas son descritas como comercios o proveedores de servicios.

### **1.2.1. COMERCIOS**

Los comercios son entidades que aceptan pagos con tarjetas de crédito, por ejemplo, el sector del comercio online, universidades, hospitales, restaurantes. [6]

<b>Nivel 1</b>
<ul style="list-style-type: none"> <li>■ Comercios cuya información de titulares de tarjeta ha estado comprometida</li> <li>■ Comercios con más de 6 millones de transacciones anuales con tarjeta de crédito</li> </ul>
<b>Nivel 2</b>
<ul style="list-style-type: none"> <li>■ Comercios con entre 1 y 6 millones de transacciones anuales con tarjeta de crédito</li> </ul>
<b>Nivel 3</b>
<ul style="list-style-type: none"> <li>■ Comercios con entre 20.000 y 1 millones de transacciones anuales con tarjeta de crédito</li> </ul>
<b>Nivel 4</b>
<ul style="list-style-type: none"> <li>■ El resto de comercios</li> </ul>

Figura 1.1. Niveles de cumplimiento de comercios. [6]

### 1.2.2. PROVEEDORES DE SERVICIO

Los proveedores de servicio son entidades que brindan servicios a los comercios, por ejemplo, empresas procesadoras de pago, pasarelas de pago, alojamiento de comercio electrónico, agencias de información de crédito. [6]

<b>Nivel 1</b>
<ul style="list-style-type: none"> <li>■ Todos los procesadores o pasarelas de pago</li> </ul>
<b>Nivel 2</b>
<ul style="list-style-type: none"> <li>■ Proveedores de servicio que no estén en el nivel 1, con más de 1 millón de cuentas/transacciones anuales con tarjeta de crédito</li> </ul>
<b>Nivel 3</b>
<ul style="list-style-type: none"> <li>■ Proveedores de servicio que no estén en el nivel 1, con menos de 1 millón de cuentas/transacciones anuales con tarjeta de crédito</li> </ul>

Figura 1.2. Niveles de cumplimiento de proveedores de servicio.

[6]



Los requerimientos para la Certificación dependen del nivel de los comercios y proveedores de servicios.

Comercio	In situ auditoría de seguridad	Auto evaluación cuestionario	Análisis de Red
Nivel 1	Requerido Anualmente		Requerido Trimestralmente
Nivel 2		Requerido Anualmente	Requerido Trimestralmente
Nivel 3		Requerido Anualmente	Requerido Trimestralmente
Nivel 4		Requerido Anualmente	Requerido Trimestralmente
Proveedor de Servicios			
Nivel 1	Requerido Anualmente		Requerido Trimestralmente
Nivel 2	Requerido Anualmente		Requerido Trimestralmente
Nivel 3		Requerido Anualmente	Requerido Trimestralmente
Por:	Asesor de Seguridad Cualificado (QSA)	Interno	Fabricante de Escáner Aprobado (ASV)
Entregable:	Informe sobre Cumplimiento (ROC)	Cuestionario de Auto Evaluación	Informe de Análisis

Figura 1.3. Procedimientos de cumplimiento PCI-DSS. [6]

### 1.3. APLICABILIDAD DE LAS PCI-DSS SOBRE LOS ELEMENTOS DE LOS DATOS DEL TITULAR DE LA TARJETA

Si no se almacena, procesa ni transmite el número de tarjeta o PAN no se aplica la norma PCI-DSS. Si el PAN se almacena, procesa o transmite, también se debe proteger los otros datos del propietario de la tarjeta según los requisitos de la norma PCI. Los datos confidenciales de autenticación no se deben almacenar después de la autorización

(incluso si están cifrados) porque con esos datos se puede generar falsas tarjetas y realizar transacciones fraudulentas. [2]

Datos de Cuentas	Elemento de datos	Almacenamiento permitido	Protección requerida	PCI-DSS req. 3, 4
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	SI	SI	SI
	Nombre del titular de la tarjeta	SI	SI	NO
	Código de servicio	SI	SI	NO
	Fecha de vencimiento	SI	SI	NO
Datos confidenciales de autenticación	Datos completos de la banda magnética o datos equivalentes que están en un chip	NO	N/A	N/A
	CAV2/CVC2/CVV2/CID	NO	N/A	N/A
	PIN/Bloqueo de PIN	NO	N/A	N/A

Figura 1.4. Datos de cuentas. [2]

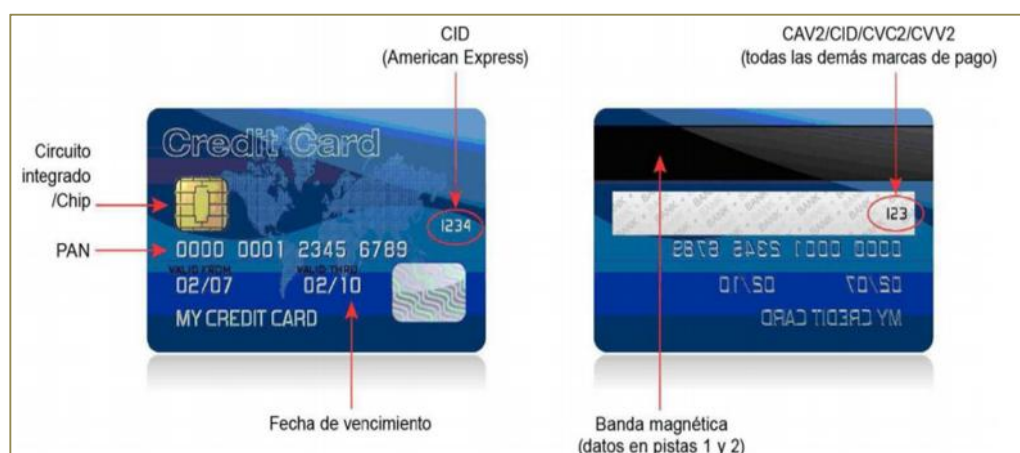


Figura 1.5. Ubicación de datos de una tarjeta de crédito. [5]

#### 1.4. REQUISITOS DE LA NORMA PCI-DSS

La norma PCI-DSS versión 1.2 fue publicado en Octubre de 2008, en abril de 2015 se actualizó a la versión 3.1 que es la que se encuentra vigente al momento de la elaboración de este trabajo en su versión sólo en inglés, se puede descargar gratuitamente a través del siguiente link:

[https://es.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-1.pdf](https://es.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf).

Esta norma agrupa doce requisitos técnicos y operativos agrupados en seis objetivos de control que sirven como referencia para proteger los datos de los titulares de tarjetas. [2]

6 Objetivos de Control	12 Requerimientos
1. Desarrollar y Mantener una Red Segura	1. Instalar y Mantener la configuración del Firewall 2. No utilizar claves ni contraseñas por defecto
2. Proteger los Datos de los Propietarios de Tarjetas	3. Proteger los datos almacenados de Tarjetahabiente 4. Cifrar los datos de tarjetahabiente enviados por redes publicas
3. Mantener un Programa de Gestión de Vulnerabilidades	5. Utilizar y Mantener un Software Antivirus 6. Desarrollar y mantener Aplicaciones Seguras
4. Implementar Medidas Solidas de Control de Acceso	7. Implementar medidas sólidas de control de acceso. 8. Identificar y autenticar el acceso a los componentes del sistema 9. Restringir el acceso Físico a los Datos
5. Monitorear (Monitorizar) y probar regularmente las redes	10. Rastrear y Monitorear todos los accesos a recursos de Red 11. Testear regularmente la Seguridad de los sistemas y Procesos
6. Mantener una Política de Seguridad de la Información	12. Mantener una Política de Seguridad de la Información

Figura 1.6. Norma de seguridad de datos de la PCI. [2]

El cumplimiento PCI es un proceso que se va mejorando con el tiempo, por lo que se puede decir que se adapta al Ciclo de Deming, es decir, cumple con la secuencia de cuatro etapas que son: [3]

- Planificar (Plan): Identificar la información sensible de las tarjetas de crédito, el flujo de datos y sus componentes, identificar qué control aplica o no de acuerdo al entorno y determinar qué acción se realizará para las excepciones. [3]
- Hacer (Do): Implementar los controles y requerimientos del estándar. [3]
- Verificar (Check): Determinar si la implementación realizada da el resultado esperado. [3]
- Actuar (Act): Corregir cualquier problema encontrado basado en la información verificada y realizar cualquier mejora que contribuya a la optimización del sistema. [3]

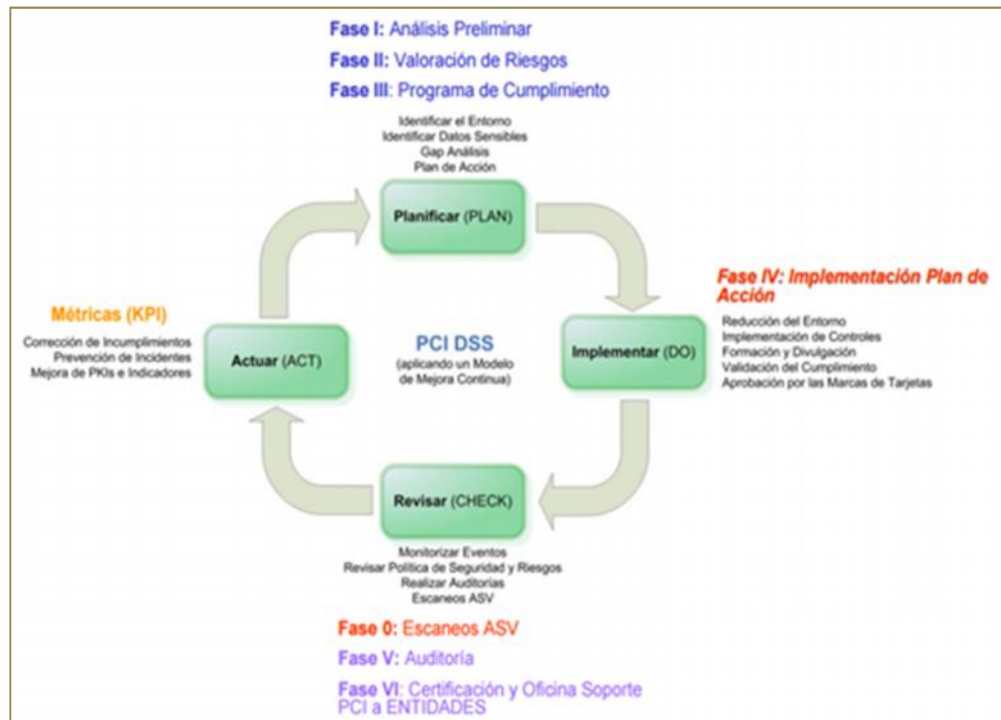


Figura 1.7. Ciclo de Deming orientado al cumplimiento de PCI-DSS. [4]

## 1.5. ASEGURAR UNA BASE DE DATOS COMO PARTE DEL CUMPLIMIENTO DE LA NORMA PCI

El estándar PCI-DSS fue creado para proteger la confidencialidad, integridad y trazabilidad de los datos relacionados con tarjetas de pago. De allí, la importancia de asegurar los componentes que forman parte del entorno de las tarjetas. No sólo es necesario asegurar los equipos de red sino que también se tiene que asegurar la base de datos, ya que es un activo fundamental que almacena información de las tarjetas de crédito.

La base de datos está expuesta a amenazas como elevación de privilegios, Inyección SQL, rastreo débil de auditorías, denegación de servicio, vulnerabilidades en el protocolo de comunicación, autenticación débil.

Los requisitos de la norma pueden ser controlados a través de la red, base de datos, acceso físico, procedimientos de control operativos, el presente trabajo está enfocado a la base de datos, lo cual compete cumplir los requisitos dos, tres, cuatro, seis, siete, ocho y diez.

## **CAPÍTULO 2**

### **METODOLOGÍA USADA**

#### **2.1. FASE I: ANÁLISIS PRELIMINAR**

Se analizó las medidas de seguridad que tenía la empresa antes de cumplir con el estándar PCI, para ver cuáles controles se cumplían parcialmente o totalmente, para esto se realizó un inventario de toda la infraestructura, ya que por ser una empresa procesadora de tarjetas, todos los componentes de la empresa son los involucrados en el entorno de tarjetas de crédito.

Antes de empezar a realizar el aseguramiento hubo reuniones con las áreas involucradas para determinar los responsables de la seguridad en los diferentes equipos y así conocer el flujo del trabajo y optimizar recursos y tiempos.

Se identificó qué servidores y aplicaciones tiene acceso cada base de datos, se comprobó que el servidor de aplicaciones y el servidor web están en diferentes servidores, el motor de base de datos está alojado en un servidor exclusivo y fue responsabilidad del administrador de servidores realizar el hardening al servidor ya que él es el responsable de dicho activo, por lo que él se encargó de deshabilitar los servicios que no correspondían a base de datos.

Así también, el servidor de base de datos no puede estar expuesto directamente a Internet, y fue responsabilidad del administrador de redes protegerlo al colocarlo en una zona desmilitarizada, configurar IPS - F5 como mecanismo de defensa perimetral, configurar en el firewall Checkpoint las reglas de acceso desde y hacia la base de datos, configurar el IPS HP TippingPoint para prevención de intrusos y protección de ataques de inyección SQL, administrar el WSUS que es el Servidor de Actualizaciones de Windows Server para considerar los parches de seguridad de SQL Server, proteger el servidor con antivirus McAfee, así como mantener actualizada la base de datos de la firma del antivirus, segmentar las redes para ambientes de desarrollo, pruebas y producción.



Como norma de seguridad tenían el servidor de base de datos, así como los otros servidores, en una área protegida, por lo que la empresa cuenta con un centro de cómputo en condiciones adecuadas para el buen estado de los servidores y accesible sólo a personas autorizadas, existen cámaras de seguridad a la entrada y dentro del centro de cómputo, equipo biométrico que permitía el paso con la huella digital, clave o tarjeta magnética, además existía la política que los operadores de centro de cómputo llevaran un registro de todo aquel que ingrese y salga del centro de cómputo por lo que siempre se enviaba un correo al operador de turno avisando la fecha y hora de entrada, fecha y hora de salida estimada, el motivo del ingreso, la o las personas que iban a ingresar, sean de la propia empresa o externos, junto con el número de cédula; dentro del centro de cómputo se encuentran claramente identificados los diferentes equipos con sus custodios en los que se incluye datos como nombres completos, cargo en la empresa, teléfono convencional y celular.

Dentro de sus políticas está el sacar respaldos diarios de la base de datos en tapes con una frecuencia de dos veces al día, que servirán como apoyo en caso de algún incidente, estos respaldos son almacenados en la cintoteca, la empresa tiene dos cintotecas, una cintoteca pequeña donde se almacena el tape o los tapes de respaldos

recientes y otra cintoteca donde se almacena respaldos más antiguos, es un cuarto con acceso restringido, sólo están autorizados ingresar el personal del área de seguridad informática y del centro de cómputo, por lo que sólo estas áreas cuentan con llaves de acceso, todo esto se encuentra documentado en el procedimiento de respaldo de información, todo esto con el fin de proteger los respaldos de accesos no deseados.

La empresa tiene dos centros de datos, uno principal ubicado en Guayaquil y otro alterno ubicado en Quito, este último fue implementado como contingencia en caso que se presente algún evento inesperado y mantener la continuidad del negocio, así también se cuenta con el procedimiento del plan de contingencia.

Existe un procedimiento para pases a producción establecido para realizar alguna operación sobre la base de datos de producción, el cual es que primero debe existir un requerimiento de desarrollo de sistema que es elaborado por el área de análisis de procesos, el cual es desarrollado por el personal de desarrollo en ambiente de desarrollo, luego se realizan pases a test y es probado por el personal de análisis de procesos en ambiente de test, una vez confirmado que está

conforme con lo realizado, a continuación se realiza el pase a producción, el mismo que debe tener la aprobación del área de Control de Calidad, se versiona los fuentes, y se verifica que el plan de ejecución de las consultas a modificar o crear no tengan costos muy altos, una vez aprobado, se realiza el pase a través de un correo electrónico.

## **2.2. FASE II: PLAN DE ACCIÓN**

Se analizó cada uno de los requisitos relacionados a bases de datos para cumplirlos o en su defecto aplicar alguna medida compensatoria.

### **2.2.1. REQUISITO 2 DE LA NORMA PCI.**

El usuario "sa" es el usuario administrador de la base de datos SQL Server con los más altos privilegios, a éste ni a ningún otro usuario, el SQL Server le asigna una clave por defecto.

### **2.2.2. REQUISITO 3 DE LA NORMA PCI.**

Para esto, SQL Server nos ofrece dos técnicas para encriptar datos:

- Encriptación de datos transparente (TDE) a nivel de toda la base de datos y
- Encriptación a nivel de celda

La encriptación TDE encripta el fichero de dato principal (.MDF) y el fichero de datos de log (.LDF); esta encriptación se usa para que en caso que se roben la base de datos, un tercero no pueda utilizar la información tratando de adjuntar los ficheros en otra instancia de SQL Server ya que necesitaría el certificado que se usó para cifrar la base de datos y/o la contraseña usada para cifrar la clave privada, TDE encripta y desencripta los ficheros en tiempo real, es decir, para guardar la página de un fichero desde la memoria a disco, guardará la página encriptada y luego para acceder, la desencriptará para cargarla a memoria.

La encriptación a nivel de celda, requiere modificar el esquema de la tabla de la(s) columna(s) que contenga(n) la información sensible, porque debe ser convertido a binario, así como las operaciones de manejo de datos, ya que al hacer una inserción se cifra y al hacer una consulta se descifra.

Para decidir cuál encriptación escoger, se consideró la transaccionalidad que realiza la empresa, en vista que es una empresa procesadora de tarjetas de crédito, realiza muchas transacciones por cada minuto, así que el realizar la operación de

cifrado y descifrado por cada transacción impactaría en el rendimiento por lo que se decidió implementar la encriptación TDE.

Como otra medida para proteger la información sensible, el número de la tarjeta se almacena en una tabla y los otros datos relacionados a la tarjeta se almacenan en otra tabla, esto para que si se llegase a comprometer sólo la tabla que contiene los números de tarjeta, al atacante no le sirva de mucho para realizar algún fraude ya que no tiene la información completa relacionada a la tarjeta.

Para propósitos de pruebas, se altera los datos de las tarjetas y sus montos en relación a los datos que están en producción, para así no comprometer dicha información para esto se adquirió un producto de terceros.

### **2.2.3. REQUISITO 4 DE LA NORMA PCI.**

SQL Server permite habilitar SSL utilizando un certificado digital, de tal modo que cuando un usuario o aplicación se conecte a nuestra Instancia SQL Server, se encripte la comunicación; sin embargo, existen herramientas que permiten encriptar el tráfico a nivel de toda la

red a través de redes virtuales privadas (VPN's) y así un tercero no podrá entender la información que se transmite.

#### **2.2.4. REQUISITO 6 DE LA NORMA PCI.**

Para esto se utilizó información de referencia de la página de Microsoft, guías de aseguramiento como CIS [8], SANS [9] [10], NSA [11], otros [12], [13] para realizar el hardening usando las mejores prácticas aplicadas al entorno.

En la configuración, la idea es evitar que personas mal intencionadas obtengan acceso o eleven privilegios, para esto a través del Sql Server Configuration Manager:

- Se desactivó los componentes y servicios de SQL Server no utilizados y se creó un usuario en el Active Directory con privilegios bajos por cada servidor para levantar los servicios de SQL Server, antes, existía un solo usuario administrador (usuario con los más altos privilegios) creado en el Active Directory, el cual levantaba todos los servicios de todos los servidores incluyendo a los servicios de SQL Server.

- Se cambió el puerto por defecto que es el 1433 y se coordinó con el administrador de redes para que modifique las reglas de acceso en el firewall.
- Se desactivó los protocolos de red no usados.

Dentro del SQL Server Management Studio se comprobó que los procedimientos extendidos almacenados no tuvieran el permiso de ejecución para el rol public, ya que este rol lo tienen todos los usuarios de la base de datos.

Se eliminó las bases de datos de prueba.

#### **2.2.5. REQUISITO 7 DE LA NORMA PCI.**

El aplicativo tiene un módulo de seguridad donde se define los roles y de acuerdo a esos roles están delimitados sus permisos, los grupos de usuarios que por sus responsabilidades, no necesitan saber el número de la tarjeta o cierta información de la tarjeta, se muestra dicha información con asterisco en el aplicativo.

### **2.2.6. REQUISITO 8 DE LA NORMA PCI.**

Como buena práctica se aconseja renombrar, deshabilitar o eliminar la cuenta "sa" que es la cuenta que tiene los más altos privilegios dentro de la base de datos SQL Server, por lo que se decidió deshabilitar esta cuenta, para evitar ataques de fuerza bruta contra esta cuenta.

La clave del usuario "sa" es guardada en un sobre cerrado protegido por una etiqueta de seguridad para evitar el manipuleo indebido y es custodiada por el área de seguridad informática, el usuario "sa" es usado sólo para labores de administración y/o configuración muy específicas que no puedan ser realizadas con otro usuario, cuando sea necesario usar el usuario "sa", se rompe el sobre para conseguir la clave, y una vez finalizada la actividad se cambia la clave del usuario sa y se vuelve a seguir el procedimiento de cuidado de claves.

Antes se usaba el usuario "sa" para realizar todas las tareas que correspondían al administrador de base de datos, tales como, administración, mantenimiento, creación de tablas, ejecución de scripts, ahora se crea un usuario para cada administrador dentro del SQL Server, cada persona es responsable de no compartir la contraseña con nadie y de cumplir los lineamientos establecidos en las



políticas de contraseñas que están definidas dentro de las políticas de seguridad de la empresa. Entre las políticas de seguridad están, que la contraseña debe cumplir con los requisitos de complejidad (mayúsculas, minúsculas, caracteres especiales), longitud mínima de ocho caracteres y la vigencia máxima de la contraseña es treinta días.

Para la creación de un nuevo usuario se fuerza el cambio de contraseña en el primer inicio de sesión, se exige las directivas de contraseña, se habilita el inicio de sesión, se verifica que no esté bloqueada la cuenta, se asigna el rol y permiso correspondientes.

Cada usuario de la aplicación tiene su propio usuario y contraseña.

Se revocó el permiso de conexión al usuario "guest" así como otros usuarios de prueba fueron eliminados.

#### **2.2.7. REQUISITO 10 DE LA NORMA PCI.**

Se decidió monitorear los siguientes eventos en la instancia de la base de datos:

- Eventos de Login exitosos y fallidos,

- Eventos de Operaciones privilegiadas como son crear, eliminar, o modificar la estructura de las tablas,
- Eventos para auditar acceso al esquema de objetos como son los SELECT,

Para esto se levantaron trazas mediante SQL Server Profiler, pero se vio que generaba una gran cantidad de registros de auditoría, por lo que posteriormente se adquirió una herramienta SIEM (Security Information and Event Management, en español significa, Seguridad de la Información y Gestión de Eventos) para recopilar y almacenar información de las auditorías.

Se adquirió el Trustwave SIEM, el cual es un appliance de hardware que permite gestionar los logs recolectados de todos los eventos de todos servidores, bases de datos, firewall, routers, fotocopiadoras; cuenta con reportes predefinidos y se puede personalizar a los ya existentes, y exportarlos en diferentes formatos, también se puede configurar alertas que pueden ser enviadas al correo cuando se detecte anomalías, por ejemplo, si se logoneó y tuvo más de cinco intentos fallidos; para que recolecte la información se instala en cada

estación el adaptador correspondiente, de esta forma se puede rastrear, analizar y evaluar la información recolectada, facilitando el estudio de la causa de algún incidente. Durante la implementación se debió tomar en consideración la sincronización de los relojes en los servidores con el fin de poder correlacionar los eventos generados por cada componente.

Como otra medida de control, la empresa instaló y configuró el OSSEC, para monitorear la integridad de los archivos, el cual alerta sobre modificaciones de configuración y contenido de archivos críticos de los distintos servidores.

Internamente, la empresa tiene personal responsable de monitorear diariamente todos los eventos de seguridad con la ayuda de las herramientas adquiridas y en caso de encontrar alguna actividad inusual que incumpla PCI, averigua la razón de tal incumplimiento con la finalidad de justificar. Por tal motivo, al procedimiento de pases a producción se agregó que entre los destinatarios del correo electrónico en el envío del pase debe estar copiado el área de seguridad informática ya que ese correo será el justificativo de porqué se modificó la estructura de la tabla.

Como medida de control de que no se esté enviando vía correo electrónico información confidencial relacionada a tarjetas de crédito, se adquirió el aplicativo Symantec Data Leak Prevention (DLP) cuyas siglas en español corresponden a prevención de pérdida de datos, el cual detecta datos sensibles, tiene una opción PCI que examina los números de la tarjeta de crédito dentro del contenido de los correos electrónicos cuando se transmiten, como parte de la configuración fue necesario, instalar el agente en todas las computadoras de la empresa (incluyendo las de Quito) y se configuró en el DLP la ip del servidor de correo, de ahora en adelante cuando se adquiere una nueva computadora como parte de los aplicativos a instalar se debe revisar que esté instalado el agente DLP.

## **CAPÍTULO 3**

### **ANÁLISIS DE RESULTADOS**

#### **3.1. HERRAMIENTAS**

Para identificar los servicios y configuración actual se puede hacer uso de herramientas para el análisis de vulnerabilidades como Microsoft SQL Server Best Practices Analyzer (BPA) que es una herramienta de diagnóstico que recopila información del servidor y la instancia de la base de datos instalada en ese servidor y determina si las configuraciones están acordes a las mejores prácticas, cuáles son los problemas y sus posibles soluciones. Esta herramienta requiere que también se instale PowerShell y Microsoft Baseline Configuration Analyzer. [7]

Otras herramientas como Nessus y Nmap informan sobre puertos, servicios habilitados, lo que permite habilitar sólo aquellos que son necesarios. Además NMAP incluye scripts que permiten realizar pruebas de penetración también llamadas "pen testing" a una base de datos SQL, por ejemplo:

- Se puede descubrir la versión del motor de base de datos,
- Validar si la cuenta "sa" no tiene contraseña,
- Realizar ataque de diccionario contra la contraseña del usuario "sa",

Si la cuenta del usuario "sa" estuviese habilitada y llegásemos a descubrir la contraseña, podríamos:

- Extraer los hashes de las contraseñas de los usuarios creados en SQL Server.
- Descubrir los nombres de las bases de datos y sus tablas y con esto realizar consultas y modificar la información directamente a la base de datos.
- Ver la configuración del motor de base de datos y si estuviese habilitado el procedimiento almacenado xp\_cmdshell, pudiéramos acceder a la interface de la línea de comando del sistema operativo y ejecutar comandos.

El uso de estas herramientas es de gran ayuda al momento de realizar el hardening, también debe referirse al sitio de la empresa del motor de base de datos ya que existe documentación específica y actualizada sobre la seguridad de los servicios, actualizaciones y parches de seguridad.

### 3.2. REPORTES PARA AUDITORÍAS

Con las auditorías almacenadas y la ayuda de una herramienta de terceros, por ejemplo, DB-Audit se puede presentar reportes como:

- **Usuarios inactivos con cuentas activas:** Se refiere a los usuarios que no se han logoneado a la base de datos, dentro del filtro del tiempo seleccionado, este reporte sirve para considerar eliminar el acceso a esos usuarios.

Tabla 2. Tabla de Usuarios Inactivos con Cuentas Activas

Nombre de Usuario	Fecha del Último Logoneo	Días Inactivos
-------------------	--------------------------	----------------

- **Usuarios que tienen privilegios Administrativos:** Este reporte muestra los usuarios de la base de datos que tienen privilegios administrativos.

Tabla 3. Tabla de Usuarios que tienen Privilegios Administrativos

Nombre de Usuario	Admin Sistema	Admin Seguridad	Admin Servidor	Admin Setup	Admin Proceso	Admin Disco	Creador de Base de Datos
-------------------	---------------	-----------------	----------------	-------------	---------------	-------------	--------------------------

- **Logins Recientes de Administrador:** Este reporte muestra todos los logins, dentro del filtro del tiempo seleccionado, cuyas cuentas tienen privilegios administrativos.

Tabla 4. Tabla de Logins Recientes de Administrador

Fecha de Login	Nombre de Usuario	Terminal	Nombre Usuario SO	Programa
----------------	-------------------	----------	-------------------	----------



- **Recientes Operaciones Privilegiadas (create, drop, alter):** Este reporte muestra todas las operaciones exitosas a nivel de objeto, dentro del filtro del tiempo seleccionado, recientemente ejecutadas, tales como: CREATE, DROP, ALTER o RENAME.

Tabla 5. Tabla de Recientes Operaciones Privilegiadas

Nombre de Usuario	Nombre Usuario SO	Fecha Evento	Acción	Base De Dato	Tipo de Objeto	Nombre de Objeto	Terminal	Programa	Comando SQL
-------------------	-------------------	--------------	--------	--------------	----------------	------------------	----------	----------	-------------

## **CONCLUSIONES Y RECOMENDACIONES**

Entre las principales conclusiones obtenidas de este trabajo se tiene que:

1. Lo más primordial para las empresas que almacenan, transmiten o procesan datos de tarjetas de crédito es conseguir el cumplimiento de la norma PCI DSS, así se evitan sanciones y altos costos de litigación, incluso podrían perder el privilegio de continuar con el procesamiento de tarjetas.
2. Las medidas de seguridad aplicadas protegen la confidencialidad, integridad y trazabilidad de la información de las tarjetas.
3. El apoyo de la dirección es un factor importante para implantar PCI-DSS, ya que exige un esfuerzo grande y mayor número de recursos.

4. Se crea una cultura de seguridad dentro de la empresa y se mejoran los procesos existentes.
5. Se debe asignar un responsable interno que lidere el proyecto de implantación de PCI-DSS, así como definir los roles y responsabilidades al personal que trabaja en el entorno PCI-DSS.
6. Se tiene identificado el entorno donde se almacena, procesa y transmite datos susceptibles de tarjetas de crédito.
7. No sólo con la acreditación de PCI-DSS o el cumplimiento de las auditorías periódicas se puede afirmar que se está cumpliendo con la norma, es necesario que los componentes del entorno cumplan con el estándar en todo momento, hay que controlar que los nuevos procesos, productos, desarrollo, compra de equipos no provoquen un incumplimiento de PCI.
8. Se debe recordar que es un plan de mejora continua, por lo que habrá que solucionar los problemas que surjan y volver a planificar si fuera necesario.

9. Es conveniente establecer un procedimiento de gestión de los cambios realizados.

Como recomendación se sugiere:

1. Elaborar el hardening primero en un ambiente de desarrollo, realizar pruebas de que funciona correctamente el aplicativo y luego aplicarlo en producción.
2. Llevar un control de los cambios que se vayan realizando para que en caso de algún problema se pueda reversar y siga operando correctamente.
3. Obtener las capturas de las evidencias de los cambios realizados mientras se realiza el hardening que servirá como pruebas para el auditor durante el proceso de auditoría.
4. Se recomienda que los logs generados, se almacenen en un servidor centralizado para realizar el análisis y facilitar la causa de algún incidente.
5. Se recomienda que todas las personas que ingresan a laborar para la empresa o empresas que brinden servicios cuyas actividades vayan a

formar parte del entorno de tarjetas firmen un acuerdo de confidencialidad.

## BIBLIOGRAFÍA

[1] Borso Elena, Normas de Seguridad PCI DSS, PA DSS y PCI PTS, <http://www.securityartwork.es/2013/01/02/normas-de-seguridad-pci-dss-pa-dss-y-pci-pts/>, fecha de publicación: 2 de enero de 2013.

[2] Security Standards Council, Requisitos y procedimientos de evaluación de seguridad Versión 3.0, [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3\\_05Nov13\\_Final\\_ES-LA.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_05Nov13_Final_ES-LA.pdf) , fecha de publicación: noviembre 2013.

[3] Acosta David, El círculo de Deming (o círculo PDCA) y la gestión de PCI DSS, <http://www.pcihispano.com/el-circulo-de-deming-o-circulo-pdca-y-la-gestion-de-pci-dss/> , fecha de publicación: 18 de junio de 2013.

[4] Internet Security Auditors (isecauditors), Proyecto: Cumplimiento estándar PCI Cumplimiento estándar PCI DSS en RSI DSS en RSI – CAJA RURAL CAJA RURAL. 2da. Jornada Seguridad Medios de Pago ITSA, [http://www.isecauditors.com/sites/default/files/files/07-01\\_PCI-DSS\\_RSI-segunda-jornada-medios-pago-itsa.pdf](http://www.isecauditors.com/sites/default/files/files/07-01_PCI-DSS_RSI-segunda-jornada-medios-pago-itsa.pdf) , fecha de publicación: noviembre de 2010.

[5] Security Standards Council, Exploración de PCI DSS - Comprensión del objetivo de los requisitos Versión 1.2, [https://es.pcisecuritystandards.org/\\_onelink\\_/pcisecurity/en2es/doc/pci\\_dss\\_saq\\_navigating\\_dss.pdf](https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/doc/pci_dss_saq_navigating_dss.pdf) , fecha de publicación: octubre de 2008.

[6] Gfihispana, El Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS), [http://www.gfihispana.com/pci/pci\\_presentation\\_es.pps](http://www.gfihispana.com/pci/pci_presentation_es.pps) , fecha de consulta: julio 2015.

[7] Microsoft Download Center, Microsoft SQL Server 2012 Best Practices Analyzer, <https://www.microsoft.com/en-us/download/details.aspx?id=29302> , fecha de consulta: julio 2015.

[8] CIS, CIS Microsoft SQL Server 2008 R2 Database v1.2.0, [https://benchmarks.cisecurity.org/tools2/sqlserver/CIS\\_Microsoft\\_SQL\\_Server\\_2008\\_R2\\_Database\\_Engine\\_Benchmark\\_v1.2.0.pdf](https://benchmarks.cisecurity.org/tools2/sqlserver/CIS_Microsoft_SQL_Server_2008_R2_Database_Engine_Benchmark_v1.2.0.pdf) , fecha de publicación: 9 de junio 2014.

[9] SANS Institute, SQL Server Security, <http://www.giac.org/paper/gsec/224/sql-server-security/100740> , fecha de consulta: julio 2015.

[10] SANS Institute, Setting Up a Database Security Logging and Monitoring Program, <https://www.giac.org/paper/gcia/960/setting-database-security-logging-monitoring-program/106192> , fecha de publicación: 10 de octubre de 2012.

[11] National Security Agency, Minimize the Effectiveness of SQL Injection Attacks, <https://www.nsa.gov/ia/files/factsheets/SqlInjectionFactSheet.pdf> , fecha de consulta: julio 2015.

[12] Berkeley Security, University of California, Database Hardening Guidelines, <https://security.berkeley.edu/node/138> , fecha de consulta: julio 2015.

[13] Ross Mistry y Hilary Cotter, Microsoft SQL Server 2008 Management and Administration, <http://cdn.ttgtmedia.com/ITKE/uploads/blogs.dir/113/files/2009/04/chapter-8->



[sql-server-2008-management-and-administration.pdf](#) , Sams Publishing, 1era.

Edición: Diciembre 2009