ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES

II PROMOCIÓN

TEMA: "MODELO DE FACTIBILIDAD PARA EL CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE DATOS EN TARJETAS DE PAGO ALINEADOS AL ESTÁNDAR PCI DSS PARA LAS ENTIDADES BANCARIAS DE ECUADOR"

AUTOR: SUNTAXI TIPAN, NELLY ROCIO

DIRECTOR: GRANDA GUTIERREZ, FAUSTO LENIN

SANGOLQUI, MARZO DE 2016

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "Modelo de factibilidad para el cumplimiento de normas de seguridad de datos en tarjetas de pago alineados al estándar PCI DSS para las entidades bancarias de Ecuador" realizado por la señora ingeniera NELLY ROCIO SUNTAXI TIPAN, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señora Ingeniera NELLY ROCIO SUNTAXI TIPAN para que lo sustente públicamente.

Quito, 24 de febrero del 2014

Atentamente

.....

FAUSTO LENIN GRANDA GUTIERREZ,
DIRECTOR DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "Modelo de factibilidad para el cumplimiento de normas de seguridad de datos en tarjetas de pago alineados al estándar PCI DSS para las entidades bancarias de Ecuador" realizado por la señora Ingeniera NELLY ROCIO SUNTAXI TIPAN, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señora Ingeniera NELLY ROCIO SUNTAXI TIPAN para que lo sustente públicamente.

Quito, 24 de febrero del 2014

Atentamente

.....

ING. RAÚL VINICIO HARO BAEZ, Msc.
PROFESOR OPONENTE DE TESIS

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, **NELLY ROCIO SUNTAXI TIPAN**, con cédula de identidad N° 1713741450, declaro que este trabajo de titulación "**MODELO DE FACTIBILIDAD PARA EL CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE DATOS EN TARJETAS DE PAGO ALINEADOS AL ESTÁNDAR PCI DSS PARA LAS ENTIDADES BANCARIAS DE ECUADOR"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.
Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Quito, 07 de marzo del 2016

.....

NELLY ROCIO SUNTAXI TIPAN
C.C. 1713741450

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES

AUTORÍZACION

Yo, **NELLY ROCIO SUNTAXI TIPAN**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "**MODELO DE FACTIBILIDAD PARA EL CUMPLIMIENTO DE NORMAS DE SEGURIDAD DE DATOS EN TARJETAS DE PAGO ALINEADOS AL ESTÁNDAR PCI DSS PARA LAS ENTIDADES BANCARIAS DE ECUADOR"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Quito, 07 de marzo del 2016

.....

NELLY ROCIO SUNTAXI TIPAN
C.C. 1713741450

DEDICATORIA

Este trabajo lo dedico a mi familia, quienes con su ejemplo han sabido enseñarme que con constancia y honestidad se pueden alcanzar todos los objetivos y metas que uno se lo propone; en especial a mi esposo Wellington quien con su apoyo, comprensión y cariño me ha llenado de entusiasmo para continuar alcanzando mis metas profesionales.

Es a ellos a quienes hoy, quiero manifestar lo importante e imprescindibles que son en mi vida.

NELLY ROCIO SUNTAXI TIPAN

AGRADECIMIENTO

Al culminar otra etapa en mi vida profesional, quiero dejar marcado mi eterna gratitud y agradecimiento a Dios, a mis padres, hermanos(as), maestros(as), a la Escuela Politécnica del Ejército y a todas las personas que de una u otra manera han sabido impulsarme y motivarme hacia la cima del éxito.

En especial un eterno agradecimiento a los Ingenieros Fausto Granda y Raúl Haro, quienes con su esmero, paciencia y dedicación han sabido transmitir sus conocimientos de una manera acertada y objetiva.

INDICE

DEDICATORIA V
AGRADECIMIENTO VI
INDICE VII
INDICE DE FIGURAS XI
INDICE DE TABLAS XII
RESUMEN XIII
ABSTRACT XIV
CAPÍTULO I 1
INTRODUCCIÓN 1
1.1 Antecedentes 1
1.2 Justificación e importancia 3
1.3 Objetivo General 4
1.4 Objetivos Específicos 4
1.5 Alcance 5
1.6 Abstract 5
1.7 Organización del documento 6
CAPÍTULO II 8
SEGURIDAD INFORMATICA 8
2.1 Generalidades 8
2.2 Definición 8
2.3 Diferencia entre Seguridad Informática y Seguridad de la Información 9
2.3.1 Seguridad Informática 9
2.3.2 Seguridad de la Información. 9
2.4 Objetivos de la Seguridad de la Información 11

2.5 Amenazas a la información 12
2.5.1. Amenazas Personas. 13
2.5.2. Amenazas Lógicas. 14
2.5.3. Catástrofes. 15
2.6 Controles de Seguridad 15
2.7 Análisis de Riesgo 16
2.7.1 Objetivos del análisis de riesgos. 17
2.8 Políticas, Planes y Procedimientos de Seguridad 17
2.8.1 Conceptos Básicos 17
2.8.2 Características Deseables de las Políticas de Seguridad. 18
2.8.3 Definición e implantación de las políticas de seguridad. 20
2.8.4 Inventario de los Recursos y Definición de los Servicios Ofrecidos……. 21
2.8.5 Realización de pruebas y auditorías periódicas. 22
2.9 Elementos de las Políticas de Seguridad 23
2.9.1 Seguridad Frente al Personal. 23
2.9.2 Adquisición de productos. 23
2.9.3 Seguridad física de las instalaciones. 24
2.9.4 Sistemas de Protección Eléctrica. 25
2.9.5 Control de nivel de Emisiones Electromagnéticas. 25
2.9.6 Vigilancia de la red y de los elementos de conectividad. 25
2.9.7 Protección en el acceso y configuración de los servidores. 26
2.9.8 Otros Aspectos. 26
2.10 Estándares de Seguridad de la Información 27
2.10.1 Otros estándares relacionados. 27
2.11 Certificaciones de Seguridad de la información 28
2.11.1 Certificaciones independientes en Seguridad de la Información…. 28
2.12 Estándar PCI DSS 28
2.12.1 Antecedentes. 28
2.12.2 Requisitos de las PCI DSS 32

2.13 PCI DSS vs ISO 27001 48
CAPÍTULO III 51
ANALISIS DE SITUACION ACTUAL 51
3.1 Antecedentes 51
3.2 Superintendencia de Bancos y Seguros 56
3.2.1 Reseña Histórica 56
3.2.2 Generalidades de la Superintendencia de Bancos y Seguros. 57
3.2.2.1 Objetivos Institucionales 57
3.2.2.2 Visión 57
3.2.2.3 Misión 57
3.2.3 Organigrama de la SBS 58
3.2.4 Entidades Bancarias del Ecuador suscritas a la SBS 61
3.3 Regulación Ecuatoriana Ajustada a los Requerimientos de PCI DSS 62
3.3.1 El Riesgo Operativo en Ecuador 63
3.3.2 SBS y la Seguridad en Canales Electrónicos 64
3.3.3 Análisis de la Normativa de la SBS y el Estándar PCI DSS. ... 66
3.3.4 Encuesta al Departamento Tecnológico de la Infraestructura Actual…… 71
3.3.4.1 Formato de Encuesta 72
3.3.4.2 Resultados de Encuesta 88
CAPÍTULO IV 92
Modelo de análisis de factibilidad de certificación PCI DSS de las entidades BANCARIAS de Ecuador 92
4.1 Elementos y datos sensibles en las tarjetas 92
4.2 Ubicación de datos sensibles de las tarjetas 94
4.3 Etapas de Aflicción en la implementación de PCI DSS 96
4.4 Dificultades para Iniciar el Proceso de Certificación 98
4.5 Dificultades en el Proceso de Certificación PCI DSS 98
4.6 Entorno de Análisis para las Entidades Bancarias 99
4.7 Entorno y términos del ámbito de las tarjetas 100

4.8 Modelo propuesto para el análisis de factibilidad de Certificación PCI DSS de Entidades Bancarias 101
4.8.1. A Quien va Dirigido el Modelo Propuesto 102
4.8.2. Detalles previos 103
4.8.3. Esquema de Implementación 104
4.8.4. Dentro de sus Propios Sistemas: 106
4.8.5. Dentro de los sistemas de los proveedores de servicios 109
4.8.6. Dentro de los Sistemas de sus Comercios 111
4.8.7. Método para Identificar Proceso de Cumplimiento en los Comercios 118
4.8.8. Estrategias de Acercamiento a PCI DSS. 121
4.8.9. Detalles del Cuestionario de Autoevaluación SAQ 123
4.9 Proceso de Auditoría del Estándar PCI DSS 124
4.10 Infraestructura de red recomendada para PCI DSS 126
4.11 Retorno de la Inversión en la Implementación PCI DSS. 128
4.11.1 Justificación de la inversión. 128
4.11.2 ROI vs ROSI 129
4.11.3 ROSI en la adecuación a PCI DSS. 130
4.11.4 Cálculo de la disminución del riesgo. 130
4.11.5 Cálculo del coste de implantar PCI DSS. 131
4.11.6 Cálculo del retorno de inversión en la implantación de PCI DSS 131
4.12 Ejemplo práctico para el cálculo del ROSI aplicado a PCI DSS 132
4.12.1 Calculo del riesgo expuesto. 132
4.12.2 Calculo del costo de implementación de PCI DSS. 135
CAPÍTULO V 137
CONCLUSIONES 137
RECOMENDACIONES 139
GLOSARIO 141
Bibliografía 145

INDICE DE FIGURAS

Figura 1 Diferencia entre Seguridad Informática y Seguridad de la Información..... 10
Figura 2 Ataques contra la seguridad de la información - Flujo normal de información entre emisor y receptor y posibles amenazas: a) interrupción; b) intercepción; c) modificación; d) creación..... 13
Figura 3 Controles de seguridad: Prevenir, detectar y recuperar..... 15
Figura 4 Políticas, Planes y Procedimientos de Seguridad..... 18
Figura 5 Programas de seguridad por marca de tarjetas..... 29
Figura 6 Establecimientos obligados a cumplir con el estándar..... 30
Figura 7 PCI DSS Categoría 1 Requisitos 1..... 33
Figura 8 PCI DSS Categoría 1 Requisitos 2..... 34
Figura 9 PCI DSS Categoría 2 Requisitos 3..... 36
Figura 10 PCI DSS Categoría 2 Requisitos 4..... 37
Figura 11 PCI DSS Categoría 3 Requisitos 5..... 38
Figura 12 PCI DSS Categoría 3 Requisitos 6..... 40
Figura 13 PCI DSS Categoría 4 Requisitos 7..... 40
Figura 14 PCI DSS Categoría 4 Requisitos 8..... 41
Figura 15 PCI DSS Categoría 4 Requisitos 9..... 43
Figura 16 PCI DSS Categoría 5 Requisitos 10..... 44
Figura 17 PCI DSS Categoría 5 Requisitos 11..... 45
Figura 18 PCI DSS Categoría 6 Requisitos 12..... 47
Figura 19 Ámbitos de ISO27001..... 48
Figura 20 Encuesta número de usuarios de Internet anual..... 51
Figura 21 Usuarios de Internet en el mundo y por nivel de desarrollo, 2001-2011..... 52

Figura 22 Usuarios de Internet en Ecuador comparativa varias fuentes..... 53
Figura 23 Usuarios con acceso a internet a nivel nacional 54
Figura 24 Uso de internet a nivel nacional 54
Figura 25 Uso de internet en Sudamérica 55
Figura 26 Organigrama SBS 60
Figura 27 Referencias de porcentajes de cumplimiento 89
Figura 28 Resultados de Encuesta 89
Figura 29 Resultados gráficos de encuesta 90
Figura 30 Datos de tarjetas 92
Figura 31 Datos de las tarjetas y su confidencialidad 94
Figura 32 Ubicación de información sensible en las tarjetas 94
Figura 33 Las 5 etapas del Aflicción de PCI DSS 96
Figura 34 Participantes del entorno de las tarjetas 101
Figura 35 Esquema de análisis para la implementación 105
Figura 36 . Pasos a seguir dentro de sus propios sistemas 106
Figura 37 Pasos a seguir dentro de los sistemas de los proveedores 109
Figura 38 Pasos a seguir dentro de los sistemas de sus comercios 111
Figura 39 Proceso de cumplimiento PCI DSS 118
Figura 40 Directrices SAQ 116
Figura 41 Topología de Red recomendada PCI DSS 126

INDICE DE TABLAS

Tabla 1 Quienes deben cumplir con la certificación PCI. 30
Tabla 2 Relación de controles ISO27001 y requisitos PCI DSS 49
Tabla 3 Características PCI DSS e ISO 27001 50
Tabla 4 Bancos Privados Nacionales activos 61
Tabla 5 Instituciones Bancarias Públicas 62
Tabla 6 Análisis de normativa SBS y PCI DSS 67
Tabla 7 Formato de Encuesta a personal de IT 72
Tabla 8 Multas VISA en caso de incidente con tarjetas de pago 133

RESUMEN

En Ecuador las entidades bancarias realizan grandes inversiones en infraestructura tecnológica encaminadas a disminuir los delitos financieros, sin embargo el porcentaje de delitos financieros no ha disminuido sino al contrario se han incrementado y la adopción de un estándar de seguridad de datos se convierte en la opción más importante a ser implementada a fin de elevar el nivel de seguridad y reducir el riesgo de pérdida de información de las tarjetas de pago sean de débito o crédito para mantener la fidelidad de sus clientes. PCI DSS es un estándar de seguridad de obligatorio cumplimiento para todas aquellas entidades que procesen, transmitan o almacenen información de tarjetas de pago, y por tanto las soluciones tecnológicas implementadas o a implementar en una entidad bancaria deben cumplir con los 12 requisitos descritos en 296 controles. El modelo de factibilidad para el cumplimiento de PCI DSS pretende guiar a todo el personal de IT para que las soluciones tecnológicas sean planteadas orientadas a cumplir los requisitos que establece PCI DSS, detalla recomendaciones técnicas, las organizaciones dependientes en el proceso, la información sobre sitios relacionados con el proceso y el análisis de justificación de la inversión que se debe realizar para obtener la certificación; pretendiendo que el momento que la entidad financiera inicie el proceso formal de certificación pueda reducir el tiempo y los costos que involucra dado que al contratar un asesor especializado QSA (Qualified Security Assessor) este realice un menor número de observaciones y cambios a ejecutar.

Palabras Claves:

- **PCI DSS**
- **SEGURIDAD EN TARJETAS DE PAGO**
- **ESTÁNDAR DE SEGURIDAD**
- **DELITOS FINANCIEROS**
- **FIREWALL PERIMETRAL**

ABSTRACT

At the Equator Banks entities, make invest heavy in technology infrastructure focus to reduce financial crime, however the percentage of financial crime hasn´t decreased. Instead that the adoption of a safety standard data becomes more important to be implemented. These do to get a safety level and risk reduction of information loss. Over all in payment cards, debit or credit card, which ensure maintain customer loyalty increasing incidents of security related to payment cards, and also the exponential growth of commercial banking transactions and the plastic makes the PCI DSS (Payment Card Industry Data Security Standard) certification one of the most important security requirements for the banking and commercial sector.

PCI DSS is a security standard mandatory for all entities that process, transmit or store payment card information, and therefore technological solutions implemented or to be implemented in a bank must comply with the 12 requirements outlined in 296 controls. The feasibility model for compliance with PCI DSS is intended to guide all IT staff for technological solutions are raised to comply the requirements of PCI DSS, Also, this detailed technical recommendations, depending of organizations in the process, Additional to this the information on sites related to the process and analysis to justify the investment must be performed to obtain certification. All of those is with the aim of financial institution initiate the formal certification process and can reduce the time and costs involved since to hire a consultant specialized QSA (Qualified Security Assessor) that make fewer comments and updates to run.

Key words:

- **PCI DSS**
- **SECURITY OF PAYMENT CARD**
- **SECURITY STANDARD**
- **FINANCIAL CRIMES**
- **PERIMETER FIREWALL**

Modelo de factibilidad para el cumplimiento de normas de seguridad de datos en tarjetas de pago alineados al estándar PCI DSS para las entidades bancarias de Ecuador.

CAPITULO I

INTRODUCCION

"La imaginación es más importante que el conocimiento. El conocimiento es limitado, mientras que la imaginación no"

— Albert Einstein

CAPÍTULO I

INTRODUCCIÓN

En la actualidad a pesar de las inversiones en infraestructura tecnológica que realizan las entidades bancarias de Ecuador, el porcentaje de delitos financieros no ha disminuido sino al contrario se ha incrementado y la adopción de un estándar de seguridad de datos se convierte en la opción más importante a ser implementada, permitiendo elevar el nivel de seguridad y reduciendo el riesgo de pérdida de información.

El aumento de la ocurrencia de incidentes de seguridad relacionados con las tarjetas de pago, sumado al crecimiento exponencial de la banca comercial y de las transacciones plásticas, hace de la certificación PCI DSS (por sus siglas en inglés: *Payment Card Industry Data Security Standard*, que significa Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago) uno de los requisitos más importantes de seguridad para el sector bancario y comercial

1.1 Antecedentes

De acuerdo a datos indicados por la Superintendencia de Bancos y Seguros “en el 2011 Ecuador contaba con 6´198.419 clientes en el sistema bancario” (Ortiz, Robalino, Benalcazar Alarcon, & Vásquez, 2012) y a pesar de las inversiones para mejorar la tecnología persiste el problema referente a fuga de información provocando perjuicio económico a los clientes. En el 2011 se registran 4869 denuncias formales a la Superintendencia de Bancos o Fiscalía respecto a delitos financieros, sin considerar el sin número de denuncias presentadas a las propias entidades bancarias las mismas que se ven obligadas a invertir recursos económicos y de personal para las validaciones y devoluciones económicas.

Estas cifras incrementan y es así que para el 2012 el número de clientes se ha incrementado a 6'792.505 (Camara de Comercio, 2012) y las denuncias formales ascienden en un 10% por año.

PCI DSS[1] es un estándar de seguridad desarrollado con el objetivo de reducir el fraude relacionado con las tarjetas de pago (débito o crédito) e incrementar la seguridad de los datos almacenados en las mismas. Este estándar es de obligado cumplimiento para todas aquellas empresas que procesen, transmitan o almacenen información de tarjetas de pago como el número de tarjeta PAN[2], fecha de caducidad, y demás información confidencial.

La adopción del estándar PCI DSS brinda beneficios ya que la entidades bancarias adquieren lineamientos que fortalecen las políticas de seguridad de datos, mejoran las prácticas de almacenamiento de la información de tarjetas de pago e información confidencial, se reducen los riesgos de compromisos masivos de tarjetas de pago, brinda mayor seguridad y confianza tanto a las marcas de tarjetas de pago como a los usuarios y en el ámbito legal reduce el riesgo de grandes multas en el caso de comprometer la información.

En Ecuador existe un bajo porcentaje de entidades bancarias que cuenten con la certificación PCI DSS provocando que incremente el riesgo de fuga de información involuntaria. Entre los problemas o riesgos más comunes, al no contar con una política de seguridad en tarjetas de pago tenemos:

- Perjuicio económico a los usuarios del servicio y la probable deserción por la falta de confiabilidad a las entidades bancarias ante el riesgo de ser víctimas de cualquiera de los tipos de delitos financieros.
- Entidades bancarias con una infraestructura tecnológica deficiente implementadas en función de soluciones de conectividad y no

[1] *Payment Card Industry Data Security Standard*: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

[2] PAN: NUMERO DE CUENTA PRINCIPAL

precautelando la seguridad de la información, convirtiéndose en organizaciones vulnerables ante intentos de penetración de intrusos.

- Inversiones económicas altas si las entidades bancarias inician el proceso de certificación en el estándar PCI DSS, dado que van a encontrarse con un sin número de observaciones y requerimientos; y, para cumplirlas deberán adecuar su infraestructura tecnológica actual para alinearse con los requerimientos definidos por el estándar (en hardware y software).

1.2 Justificación e importancia

En Ecuador solo existe una entidad bancaria que cuentan con certificación PCI DSS[3], dos entidades bancarias iniciaron el proceso de certificación en el 2012, evidenciando el bajo porcentaje de entidades bancarias suscritas a la Superintendencia de Bancos y Seguros que cuenten con una certificación internacional en el ámbito de la seguridad. De contar con esta certificación ayudaría a reducir el fraude relacionado con las tarjetas de pago (crédito o débito), ya que el estándar busca incrementar la seguridad de los datos almacenados en las mismas.

La adopción del estándar de seguridad de datos PCI DSS se convierte en una de las herramientas más importantes a implementar por las instituciones financieras en nuestro país, permitiéndoles elevar su nivel de seguridad y reducción del riesgo de compromiso de la información sensible de las tarjetas de pago.

Es necesaria la adopción de estándares de seguridad que estén difundidos a nivel mundial para el uso y manejo de canales electrónicos de manera de poder realizar transferencias seguras de información confidencial.

[3] *Payment Card Industry Data Security Standard*: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

El fraude haciendo uso de tarjetas de pago ha encontrado mayor rédito económico al comprometer los datos de miles de tarjetas a los que logran acceder a causa de las malas prácticas de seguridad de información que es el común de varias organizaciones a nivel nacional. Las normas de seguridad de datos emitidas por PCI DSS son orientadas a establecer una base firme y estructurada de seguridad que pretende reducir notablemente los altos riesgos de seguridad propio del uso de tarjetas de pago y evitar fraudes masivos que perjudiquen con grades sumas económicas a los tarjeta habientes.

Se pretende definir un modelo para que las entidades bancarias se encaminen en el proceso de certificación de manera que las observaciones sean mínimas y reduzcan el tiempo de ejecución; y este modelo sea tomado como referente a todas las entidades bancarias obligadas a cumplir con este requerimiento.

1.3 Objetivo General

Plantear un modelo de factibilidad para el cumplimiento de la seguridad de datos en las tarjetas de pago alineados al estándar PCI DSS[4] en las entidades bancarias de Ecuador con la finalidad de fortalecer la seguridad de las transacciones.

1.4 Objetivos Específicos

a) Analizar la situación actual de una entidad bancaria de Ecuador y describir las recomendaciones que se deberían ejecutar previas a iniciar el proceso de certificación en el estándar PCI DSS, a fin de verificar la situación actual respecto a las normas establecidas y el nivel de cumplimiento frente a la regulación ecuatoriana sobre delitos financieros.

[4] *Payment Card Industry Data Security Standard*: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

b) Documentar las mejores prácticas de seguridad y políticas relacionadas a la seguridad informática que se deben implementar en la infraestructura tecnológica de manera que se inicie un proceso para cumplir con los requerimientos del estándar PCI DSS encaminados en una futura certificación en el estándar.
c) Presentar un modelo de factibilidad técnica y económica para la ejecución del proceso de certificación en el estándar PCI DSS en las entidades bancarias.

1.5 Alcance

Dado que la norma PCI DSS es aplicable a todas las entidades en las cuales se procesa, transmite y almacena información de tarjetas de pago su alcance es muy amplio, de manera que la presente tesis considerará únicamente a los Bancos del Ecuador excluyendo del análisis a las cooperativas y mutualistas.

1.6 Abstract

At the Equator Banks entities, make invest heavy in technology infrastructure focus to reduce financial crime, however the percentage of financial crime hasn´t decreased. Instead that the adoption of a safety standard data becomes more important to be implemented. These do to get a safety level and risk reduction of information loss. Over all in payment cards, debit or credit card, which ensure maintain customer loyalty Increasing incidents of security related to payment cards, and also the exponential growth of commercial banking transactions and the plastic makes the PCI DSS (Payment Card Industry Data Security Standard) certification one of the most important requirements security for the banking and commercial sector. By 2012 the number of clients in the banking sector has increased to 6'792 .505 and formal complaints rise by 10% per year (Camara de Comercio, 2012) .

PCI DSS is a security standard mandatory for all entities that process, transmit or store payment card information, and therefore technological solutions implemented or to be implemented in a bank must comply with the 12 requirements outlined in 296 controls. PCI DSS is designed to reduce security risks specific to the use of payment cards to avoid being part of massive fraud that causes economic damage to the owners thereof.

PCI DSS don´t replace the local laws and regulations, for this reason was necessary a studio comparative analysis with the rules set by regulatory entity at Equator, Superintendence of Banks and Insurance which comply with safety guidelines defined international standards.

The feasibility model for compliance with PCI DSS is intended to guide all IT staff for technological solutions are raised to comply the requirements of PCI DSS, Also, this detailed technical recommendations, depending of organizations in the process, Additional to this the information on sites related to the process and analysis to justify the investment must be performed to obtain certification.

All of those is with the aim of financial institution initiate the formal certification process and can reduce the time and costs involved since to hire a consultant specialized QSA (Qualified Security Assessor) that make fewer comments and updates to run.

1.7 Organización del documento

Para un mejor entendimiento de la estructura del documento, brevemente se menciona su contenido general:

- Capítulo I, describe de manera general la justificación, objetivos y alcance del documento.

- Capitulo II, describe los conceptos generales referentes a la seguridad de la información, la seguridad informática, estándares relacionados y detalla los requisitos específicos del estándar PCI DSS.
- Capitulo III, describe la situación actual respecto a los estándares de seguridad de la información establecidos por el ente regulador en Ecuador (Superintendencia de Bancos y Seguros) y presenta los resultados de la encuesta realizada a entidades bancarias.
- Capitulo IV, describe modelo propuesto para analizar la factibilidad de certificación PCI DSS de las entidades bancarias en Ecuador.
- Capítulo V, describe las conclusiones y recomendaciones como resultado del análisis realizado en los capítulos anteriores.

Modelo de factibilidad para el cumplimiento de normas de seguridad de datos en tarjetas de pago alineados al estándar PCI DSS para las entidades bancarias de Ecuador

CAPITULO II

SEGURIDAD INFORMATICA

Si piensa que la tecnología puede solventar sus problemas de seguridad, entonces no entiende los problemas de seguridad ni entiende la tecnología.

Bruce Schneier " Secrets and Lies.
Digital Security in a Networked World, 2000 ".

CAPÍTULO II

SEGURIDAD INFORMATICA

2.1Generalidades

La informática se ha extendido en todos los ámbitos del ser humano, pero paralelamente al uso de la informática y las redes de comunicaciones se multiplican los incidentes de seguridad. Todas las empresas grandes o pequeñas realizan una inversión en seguridad lo que indica que todas son conscientes de la amenaza a las que se exponen. Con el fin de dirigir eficientemente estos esfuerzos de protección se vuelve imprescindible analizar un mínimo ejercicio de análisis de riesgo que permitan identificar los activos prioritarios a proteger, frente a qué amenazas y con qué riesgos.

Si no se toma ninguna medida de protección, la información está expuesta a amenazas con una probabilidad de ocurrencia y un riesgo asociados. Se hace necesario evaluar los riesgos reales a los cuales están expuestos y mitigarlos con la aplicación de medidas necesarias y en el grado adecuado que implique la participación coordinada de tecnología, personas y operaciones. No se busca conseguir sistemas 100% seguros, sino sistemas tan seguros como sea necesario para proteger los activos de acuerdo a las expectativas planteadas y que actúen de acuerdo a las amenazas actuales.

2.2Definición

Según Vieites:

La seguridad informática, se enfoca en la protección de la infraestructura computacional y todo lo relacionado incluyendo la información contenida. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, archivos y todo lo que la organización valore y

significique un riesgo si esta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial. (Vieites Á, 2007)

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. Por tal razón revisemos la definición de los dos términos para diferenciarlos:

2.3Diferencia entre Seguridad Informática y Seguridad de la Información

2.3.1Seguridad Informática

Se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (se centra básicamente en hardware y software), y que estas sean utilizadas de la manera indicada por la Organización. Su análisis de riesgos se centra en vulnerabilidades del hardware o software, y además llevar el nivel de riesgo a nivel aceptable por la organización.

2.3.2Seguridad de la Información.

La seguridad de la información tiene como propósito proteger la información de una Organización, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

La Seguridad de la Información tiene tres principios fundamentales: Confidencialidad, Integridad y Disponibilidad de la información, a través de medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información. Su

radio de acción cubre: Análisis de Riesgos, Seguridad del Personal, Seguridad física y del entorno, Gestión de comunicaciones, Desarrollo y Mantenimiento de Sistemas, Control de Accesos, Gestión de Incidentes, y Continuidad de Negocio entre otros (de acuerdo a la ISO 27000).

En la figura 1, se puede observar con mayor claridad la diferencia del alcance de la seguridad de la información y seguridad informática. Todas las áreas aquí ilustradas se encuentran dentro del alcance de la seguridad de la información de acuerdo al estándar ISO 27000, pero las áreas con color amarillo son las que se encuentran dentro del alcance de la seguridad informática (dependiendo de los recursos con los que cuente la Organización); claro que esto puede estar sujeto a infinidad de discusiones pero es evidente que el alcance de la seguridad de la información es mucho más amplio que el de la seguridad informática. (Council S. S., 2012)

Figura 1 Diferencia entre Seguridad Informática y Seguridad de la Información.

Fuente: (Palma, 2011)

2.4Objetivos de la Seguridad de la Información

La Seguridad de la información es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información en una entidad; y sus objetivos principales de acuerdo a Vieitis son (Vieites Á, 2007):

- Minimizar, gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes que ingresan esta información en sus contratos.

Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación:

- Técnico, tanto a nivel físico como lógico
- Legal, algunos países obligan por ley a que en determinados sectores se implanten una serie de medidas de seguridad. En Ecuador, el sector de servicios financieros a través de la Superintendencia de Bancos y Seguros (SBS)[5] (SuperIntendencia de Bancos y Seguros, 2012)
- Humano, sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal.

[5] http://www.sbs.gob.ec/

- Organizativo, definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

2.5 Amenazas a la información

Las amenazas a la información se dividen en cuatro grupos o categorías. En función de la figura 2 podemos explicar cada grupo considerando que la información “I” debe llegar del punto A hacia B en un flujo normal:

- Creación de la información (d): si se penetra nueva información dentro del sistema se está atentando contra la seguridad. Por ejemplo la creación de una cuenta inexistente en un banco o la adición de registros a una base de datos. En este caso en el punto B se crea información adicional I+I1.
- Modificación de información (c): La información I enviada por A llega a B pero con alteraciones en la misma “i”. Como ejemplo podemos citar el cambio de valores de un archivo de datos, manipular un programa para que funcione de forma diferente o modificar el contenido de un mensaje que están siendo transferidos por la red.
- Intercepción de información (b): La Información I enviada por A llega al punto B pero también es obtenida por C. Como por ejemplo interceptar una línea y se podría manejar los datos que están en la red, la copia ilícita de ficheros y programas secretos.
- Interrupción de la información (a): Los ataques también pueden alterar la disponibilidad de los datos alojados en los sistemas o los que viajan por las redes de comunicaciones. La información I enviada por A probablemente nunca llegue a B. Por ejemplo está la destrucción de un elemento hardware como un disco o el corte de un enlace de comunicación.

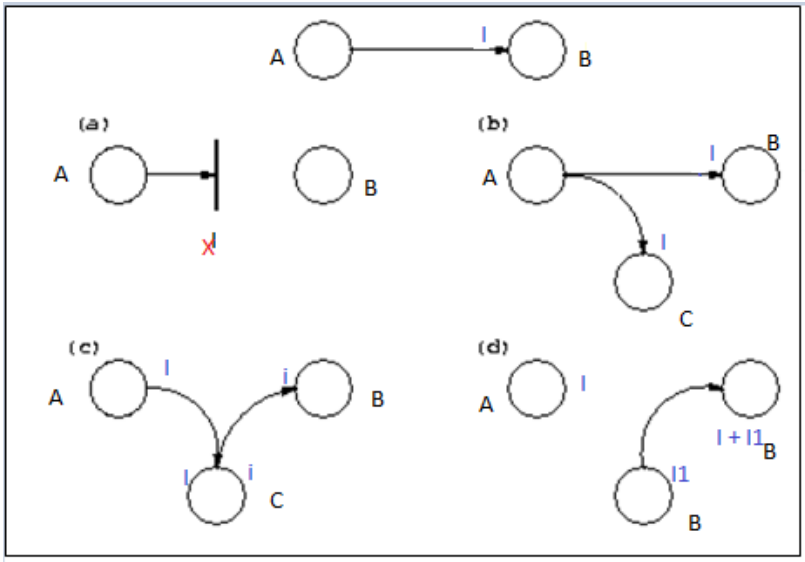


Figura 2 Ataques contra la seguridad de la información - Flujo normal de información entre emisor y receptor y posibles amenazas: a) interrupción; b) intercepción; c) modificación; d) creación

Fuente: (Palma, 2011)

A continuación se detalla una relación de los elementos que potencialmente constituyen una amenaza con el fin de tener una idea de qué o quién es una amenaza a nuestros sistemas:

2.5.1. Amenazas Personas.

La mayoría de ataques a los sistemas provienen de personas que intencionada o inintencionadamente pueden causar enormes pérdidas, se la puede dividir en dos grupos: atacantes pasivos, aquellos que aceden al sistema pero no lo modifican o destruyen como los curiosos o crackers; y los activos, aquellos que dañan el objetivo atacado o lo modifican a su favor como los terroristas y ex empleados. Por tanto aquí podemos mencionar como amenazas:

- Personal
- Ex-empleados
- Curiosos

- Crackers
- Terroristas
- Intrusos (remunerados)

2.5.2.Amenazas Lógicas.

Encontramos todo tipo de programas que de una u otra forma pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso o malware) o simplemente por error (bugs o agujeros); así tenemos:

- Software incorrecto: se debe a errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.
- Herramientas de seguridad: de igual manera que se las utiliza para detectar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos fallos y aprovecharlos para atacar.
- Puertas traseras: los programadores en el desarrollo de grandes o complejos sistemas suelen insertar atajos denominados puertas traseras y si estos atajos se los mantiene en versiones definitivas de un software y es descubierta por un atacante va a tener acceso global a datos que no debería poder leer.
- Bombas lógicas: son parte del código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas a través de la ausencia o presencia de ciertos ficheros, la llegada de una fecha concreta; al activarse se podrá realizar cualquier tarea y los efectos pueden ser fatales.
- Virus: a través de secuencia de códigos que se insertan en un fichero ejecutable (huésped) de manera que cuando se ejecuta, el virus también se ejecuta insertándose en otros programas.
- Gusanos: es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.

- Caballo de Troya: son instrucciones escondidas de un programa de forma que éste parezca realizar tareas que un usuario espera de él pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.

2.5.3.Catástrofes.

Pueden ser naturales o artificiales y son amenazas menos probables ya que depende de varios factores como la ubicación geográfica. A pesar de que son menos probables, no se está exento de un terremoto o inundación y se deben tomar medidas de contingencia.

2.6Controles de Seguridad

Como parte de la seguridad deben implantarse los tres tipos de medidas coordinadamente: Prevención, Detección y Recuperación. Dada la realimentación que se establece entre ellas como se muestra en la figura 3: la prevención evita el tener que recurrir a la recuperación, mientras que la detección facilita la recuperación y realimenta la prevención.

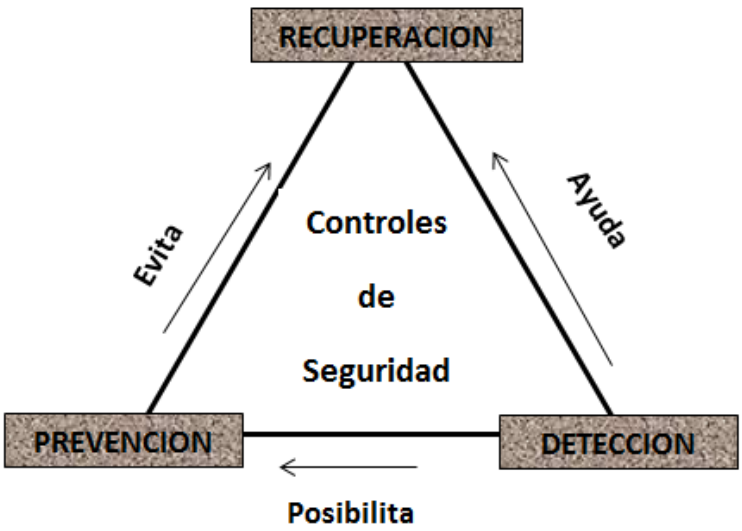


Figura 3 Controles de seguridad: Prevenir, detectar y recuperar.

Fuente: (Vieites Á, 2007)

Todos los productos de seguridad informática existentes en el mercado cumplen básicamente las siguientes funciones:

- Prevenir: Aumentar el nivel de seguridad de manera que evita que los ataques tengan éxito. Como ejemplo podemos mencionar a los firewalls.
- Detectar: Alerta cuando se produce una anomalía debido a un intruso. Por ejemplo los IDS (*Intrusion Detection System*).
- Recuperar: Garantiza que ante un incidente de seguridad, causado o fortuito se pueda recuperar toda la información y retornar a la normalidad en un tiempo mínimo. Como ejemplo podemos mencionar las copias de seguridad.

2.7Análisis de Riesgo

Es el primer paso que se debe tomar en cuenta para implementar la seguridad de la información. El análisis de riesgos identificará las amenazas asociadas a cada uno de los procesos de negocio, activos de información, la probabilidad de ocurrencia la vulnerabilidad ante esas amenazas y se estimará el impacto de una falla de seguridad dentro de la entidad.

Los riesgos son valorados en términos de la probabilidad de ocurrencia y el impacto potencial causado por la pérdida de confidencialidad, integridad y disponibilidad de los activos de información. Los beneficios del análisis de riesgos son:

- Identificación objetiva de los procesos y activos de información críticos que impactan en la continuidad del negocio.
- Evaluación de la eficacia de los controles y procesos de seguridad implantados.
- Optimizar las futuras inversiones en seguridad.
- Seguimiento y control de la evolución de los niveles de riesgo de la organización.

"Las metodologías conocidas[6] para el análisis de riesgos en el ámbito de la Seguridad Informática son: Magerit, Octave y Mehari." (Eterovic & Pagliari , 2011)

2.7.1Objetivos del análisis de riesgos.

Se plantea los siguientes objetivos:

- Evaluar y manejar los riesgos de seguridad.
- Tomar las mejores decisiones en seguridad informática
- Enfocar los esfuerzos en la protección de los activos.

2.8Políticas, Planes y Procedimientos de Seguridad

2.8.1Conceptos Básicos.

Según Vieites, a continuación detallamos conceptos básicos sobre Políticas, Planes y Procedimientos de seguridad para poder diferenciar cada término:

- Podemos definir una **Política de Seguridad** como una "declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran". (Eterovic & Pagliari , 2011)
- Un **Plan de seguridad** es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.
- Un **Procedimiento de seguridad** es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización. (Vieites Á, 2007)

[6] http://www.cyta.com.ar/ta1001/v10n1a3.htm

Figura 4 Políticas, Planes y Procedimientos de Seguridad.

Fuente: (Vieites Á, 2007)

La figura 4 representa la jerarquía de los conceptos descritos. En este sentido, las Políticas definen "qué" se debe proteger en el sistema, mientras que los Procedimientos de Seguridad describen "cómo" se debe conseguir dicha protección. En definitiva, si comparamos las Políticas de Seguridad con las Leyes en un Estado de Derecho, los procedimientos serían el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes.

2.8.2Características Deseables de las Políticas de Seguridad.

Se presenta de forma esquemática las principales características y requisitos que debería cumplir las Políticas de Seguridad, según Palma:

- Las políticas de seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas de hardware que implanten servicios de seguridad.

- Deben definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la entidad.
- Debe cumplir con las exigencias del entorno legal.
- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. La periodicidad debe ser definida en función de las necesidades de cada organización.
- Aplicación del principio de "Defensa en profundidad": definición e implantación de varios niveles o capas de seguridad.
- Asignación de los mínimos privilegios: los servicios, las aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.
- Configuración robusta ante fallos (en hardware y software): los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.
- Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros, sino que deberían estar adaptadas a las necesidades reales de cada entidad. (Palma, 2011)

Es necesario tener en cuenta una serie de dificultades a la hora de definir las Políticas de Seguridad y considerar que en gran porcentaje los problemas inherentes a la seguridad se producen por fallos en los equipos o por un mal uso de las políticas de seguridad por parte del personal de la propia entidad.

2.8.3Definición e implantación de las políticas de seguridad.

Al definir las Políticas de Seguridad en una entidad se debe contemplar los aspectos enumerados a continuación:

- Alcance: recursos, instalaciones y procesos de la entidad sobre los que se aplican.
- Objetivos perseguidos y prioridades de seguridad.
- Compromiso de la Dirección de la entidad.
- Clasificación de la información e identificación de los activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes involucrados en la implantación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles organizacionales.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos por parte del personal (Appropiate User Policy)
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de las relaciones con terceros (clientes, proveedores, socios)
- Gestión de incidentes.
- Planes de contingencia y de continuidad del negocio.
- Cumplimiento de la legislación vigente.
- Definición de las posibles violaciones y de las consecuencias derivadas del incumplimiento de las políticas de seguridad.

Las personas o miembros que intervienen en la definición de las Políticas de Seguridad dentro de la entidad son:

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del Departamento de Informática y Comunicaciones.
- Miembros del Equipo de Respuesta a Incidentes de Seguridad Informática (*CSIRT, Computer Security Incident Response Team*), en caso de que éste exista.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en seguridad informática.

Es importante la difusión de las Políticas de Seguridad y su claro conocimiento de los miembros de la entidad a través de ejemplos que faciliten su comprensión. Debe existir documentación clara y detallada sobre todas las directrices de seguridad, de fácil entendimiento y que contengan toda la información que permitan identificar autores, acciones, eventos, fechas de ejecución, responsables.

2.8.4 Inventario de los Recursos y Definición de los Servicios Ofrecidos.

La implementación de los distintos elementos de las Políticas de Seguridad requiere de un inventario previo y del mantenimiento de un registro actualizado de los recursos del sistema informático de la entidad: equipamiento de hardware y de comunicaciones, software, datos, documentación, manuales, consumibles, etc.

Se debe identificar los distintos puntos de acceso a la red y los tipos de conexiones utilizadas. Mantener el inventario de los recursos facilitara el posterior análisis de las vulnerabilidades del sistema informático, identificando los posibles objetivos de ataques o intentos de intrusión.

2.8.5 Realización de pruebas y auditorías periódicas.

La realización de pruebas y auditorías periódicas de seguridad constituyen un elemento de gran importancia para poder comprobar la adecuada implantación de las directrices y medidas definidas en las Políticas de Seguridad. Se recomienda que dichas pruebas o auditorias sean ejecutadas al menos 1 vez cada semestre, las pruebas de seguridad que se pueden realizar son:

- Análisis de posibles vulnerabilidades del sistema informático, empleando herramientas como Nessus o Internet Security Scanner para tratar de localizar de forma automática algunas de las vulnerabilidades más conocidas.
- Sondeos de seguridad que complementan el análisis de vulnerabilidades con tareas de detección y de revisión de la instalación y configuración de los equipos de seguridad (firewalls, antivirus, IDS, entre ellos).
- Pruebas de intrusión, en las que no sólo se detectan las vulnerabilidades, sino que se trata de explotar las que se hayan identificado para tratar de comprometer el sistema afectado.
- Otras pruebas de seguridad que contemplan aspectos humanos y organizacionales, recurriendo a técnicas como la "Ingeniería Social" para tratar de descubrir información sensible o determinados detalles sobre la configuración y el funcionamiento del sistema.
- El análisis y evaluación de riesgos, en el que se pretende determinar cuál es el nivel de riesgo asumido por la entidad a partir del análisis de posibles amenazas y vulnerabilidades.

Es importante como parte de estas pruebas validar la adecuada ejecución de los planes de contingencia y como parte de las auditorias se debe revisar el nivel de cumplimiento de los requisitos legales.

2.9Elementos de las Políticas de Seguridad

A continuación se detalla los distintos aspectos a tener en cuenta dentro de cada uno de los elementos de las Políticas de seguridad relacionados con la seguridad de la información y del sistema informático de una entidad.

2.9.1 Seguridad Frente al Personal.

2.9.1.1 Alta de empleados.

- Prestar atención y revisar referencias.
- Firma de contratos de confidencialidad cuando los datos sean sensibles.
- Definir el procedimiento para la creación de cuentas de usuario dentro del sistema. (identificación y autenticación)
- Establecer derechos, obligaciones y responsabilidades en relación con la seguridad de los datos y las aplicaciones.

2.9.1.2 Baja de empleados.

- Definir el procedimiento de eliminación o bloqueo de cuentas.
- Revocación de permisos y privilegios.
- Devolución de equipos, tarjetas y otros dispositivos.

2.9.1.3 Funciones, obligaciones y derechos de los usuarios.

- Definir niveles de acceso a los servicios y recursos.
- Creación de cuentas de usuarios y asignación de permisos de acceso.
- Segregación de responsabilidades.
- Definir posibles violaciones a las Políticas de Seguridad y las consecuencias para los responsables.
- Sensibilización a los usuarios.

2.9.2Adquisición de productos.

- Evaluación de productos de acuerdo a las necesidades y requisitos del sistema, características técnicas, características de seguridad, costo-beneficio, fabricante, etc.

- Evaluación de proveedores.
- Comparativos de ofertas.
- Términos y condiciones de compra.
- Instalación y configuración de productos.
- Formación y soporte a usuarios (incluyendo el personal técnico).
- Tareas de soporte y mantenimiento postventa.
- Actualización de productos con nuevas versiones y parches de seguridad.

2.9.3Seguridad física de las instalaciones.

- Protección frente a daños por fuego, inundación, explosiones, accesos no autorizados, etc.
- Selección de elementos constructivos internos más adecuados: puertas, paredes, suelos y techos falsos, canalizaciones eléctricas y de comunicaciones.
- Definición de distintas áreas o zonas de seguridad dentro del edificio:
    - **Áreas públicas**: pueden acceder sin restricciones personas ajenas a la organización.
    - **Áreas internas**: reservadas a los empleados
    - **Áreas de acceso restringido**: áreas críticas a las que sólo pueden acceder un grupo reducido de empleados con el nivel de autorización requerido.
- Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.
- Implantación de sistemas de vigilancia basados en cámaras de CCTV (Circuito Cerrado de Televisión), alarmas y detectores de movimiento.
- Control de condiciones ambientales en las instalaciones, mediante un sistema independiente de ventilación, calefacción, aire acondicionado y humidificación/deshumidificación (*HVAC: Heating, Ventilating and Air Conditioning System*), en un esquema 24x7.

- Cerraduras, candados y mecanismos de anclajes de equipos.
- Firmas de contratos o bitácoras de entrada y salidas al "site" o "data center".

2.9.4Sistemas de Protección Eléctrica.

- Adecuada conexión de los equipos a la toma de tierra.
- Revisión de instalación eléctrica específica para el sistema informático, aislada del resto de la instalación eléctrica de la organización.
- Filtrado de ruidos e interferencias electromagnéticas que pueden afectar el normal funcionamiento de los equipos.
- Utilización de Sistemas de Alimentación Ininterrumpida (UPS).

2.9.5Control de nivel de Emisiones Electromagnéticas.

Todos los equipos informáticos y electrónicos emiten señales radioeléctricas que podrían revelar información de interés a aquellos usuarios con los medios para interceptar y analizar dichas señales. Bastaría una antena direccional, amplificadores y equipos de radiofrecuencia conectados a una computadora.

- Esto puede hacerse para duplicar la imagen de monitores.
- Información escrita en discos duros o bien enviada a través de la red.
- Se debe a un estándar que defina: Aislamiento, Filtros, uso de fibra óptica o cables apantallados.

2.9.6 Vigilancia de la red y de los elementos de conectividad.

- Proteger o blindar dispositivos de red, como los hubs, switches, routers o puntos de acceso inalámbricos para impedir accesos no autorizados.

- Se pueden recurrir a medidas extremas como tubos con aire a presión o reflexómetros.

2.9.7Protección en el acceso y configuración de los servidores.

- Utilizar contraseñas de acceso.
- Separación de servicios críticos.
- Respaldos.
- Configuración más segura y robusta en los servidores.

2.9.8Otros Aspectos.

Otros aspectos a considerar son:

- Protección en los equipos y estaciones de trabajo.
- Control de equipos que puedan salir de la entidad.
- Copias de seguridad.
- Control de la seguridad de impresoras y otros dispositivos periféricos.
- Borrado de información.
- Autorización y control de acceso.
- Protección de datos y documentos sensibles.
- Auditoría a la administración de la seguridad.

Se ha revisado todos los elementos que intervienen en las Políticas de Seguridad y la implantación de adecuadas medidas de seguridad informática que exige contemplar aspectos técnicos pero se debe considerar la importancia del factor humano en la seguridad informática.

Dado que nuestro interés es la protección de los datos almacenados, transmitidos o procesados en las tarjetas de pago y específicamente el estándar PCI DSS, revisemos algunos estándares y certificaciones.

2.10Estándares de Seguridad de la Información

Entre los estándares de seguridad de la información podemos mencionar:

- ISO/IEC 27000-series: La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Existen varias versiones.

- ISO/IEC 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

- ISO/IEC 17799: Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

2.10.1Otros estándares relacionados.

- COBIT: es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: *Information Systems Audit and Control Association*), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: *IT Governance Institute*) en 1992.

- ITIL: es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de

tecnologías de la información y las operaciones relacionadas con la misma en general.

2.11Certificaciones de Seguridad de la información

Las certificaciones existentes y que se debe validar su factibilidad en función de los objetivos de cada entidad son:

- CISM - CISM Certificaciones: Certified Information Security Manager
- CISSP - CISSP Certificaciones: *Security Professional Certification*
- GIAC - GIAC Certificaciones: *Global Information Assurance Certification*

2.11.1Certificaciones independientes en Seguridad de la Información.

- *CISA- Certified Information Systems Auditor*, ISACA
- CISM- Certified Information Security Manager, ISACA
- *Lead Auditor* ISO27001- *Lead Auditor* ISO 27001, BSI
- CISSP - Certified Information Systems Security Professional, ISC2
- SECURITY+, COMPTia - *Computing Technology Industry Association*
- CEH - *Certified Ethical Hacker*
- PCI DSS - PCI *Data Security Standard*

2.12 Estándar PCI DSS

2.12.1 Antecedentes.

Con el fin de concentrar los esfuerzos para minimizar el riesgo de fraudes con tarjetas de pago, los grandes operadores mundiales se han asociado en la organización denominada PCI SSC “*Payment Card Industry Security Standards Council*. (Council P. S., 2012) Algunos de sus miembros son:

• VISA
• DINERS
• MASTERCARD
• DISCOVER CARD
• AMERCIAN EXPRESS
• JCB

La organización fue creada en septiembre de 2006 para coordinar y administrar acciones relativas a la seguridad de la información relacionada a tarjetas de pago y sus titulares. Hasta antes de esta fecha cada marca de tarjetas tenía su propio programa de requerimientos de seguridad, es decir no existía una coordinación y esto lo evidenciamos en la figura 5.

Las funciones del PCI-SSC son las siguientes:

• Definir, desarrollar, mantener y distribuir el "*PCI Data Security Standard" (PCI-DSS)*
• Entrenar, testear y certificar *Qualified Security Asessors (QSAs)*
• Entrenar, testear y certificar *Approved Scanning Vendors (ASVs)*

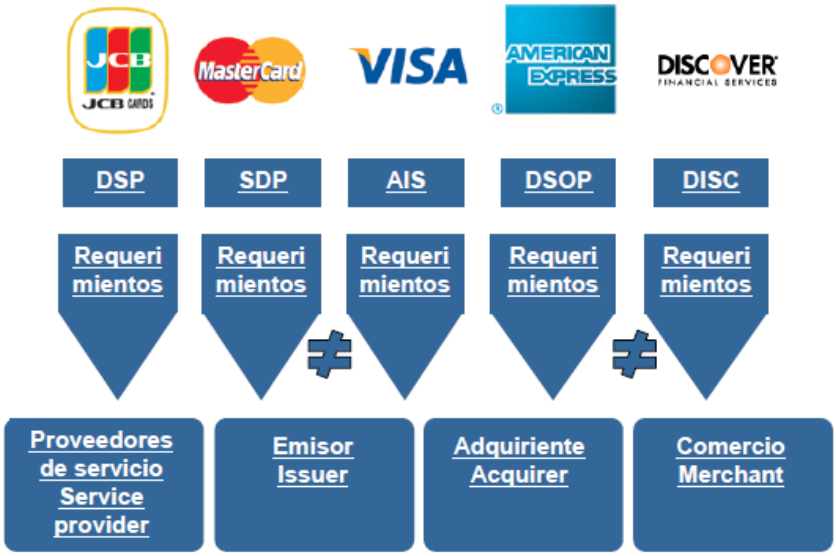


Figura 5 Programas de seguridad por marca de tarjetas

Fuente: (Council P. S., 2012)

El criterio para determinar quién debe cumplir con PCI es muy sencillo: deberán hacerlo siempre que transmitan, procesen o almacenen datos de tarjetas de pago. Por lo general, estos establecimientos caen en comercios minoristas, bancos, e-commerce y proveedores de servicios. En la figura 6, se identifica quienes deben demostrar el cumplimiento del estándar:

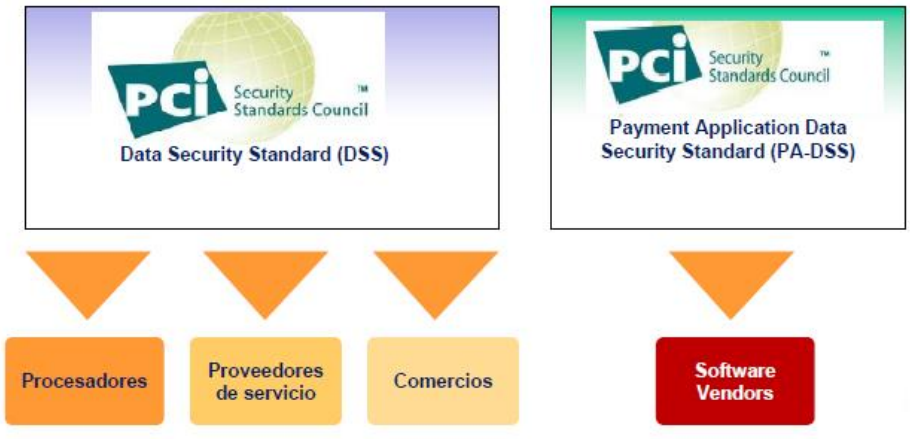


Figura 6 Establecimientos obligados a cumplir con el estándar.

Fuente: (Council P. S., 2012)

En la tabla 1, se detalla características para especificar quienes deben certificarse en función del número de transacciones anuales:

Tabla 1

Quienes deben cumplir con la certificación PCI.

PCI–DSS - Procesadores y proveedores de servicios		
	VISA	**MASTERCARD**
1 300.000	Procesadores de VisaNet o cualquier proveedor de servicio que almacene, procese o transmita más de 300.000 transacciones anualmente	Todos los TPP (Third Party Processor) Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan más de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro

Continua

2	Cualquier proveedor de servicio que almacene, procese o transmita menos de 300.000 transacciones Anualmente	Todos los DSE (Data Storage Entities) que almacenen, procesen o transmitan menos de 300.000 transacciones anualmente combinadas entre MasterCard y Maestro
PCI-DSS – Comercios		
1 6 000.000	Más de 6 millones de transacciones anuales de VISA o comercios globales identificados como Nivel 1 por VISA fuera de USA.	Más de 6 millones de transacciones MasterCard anualmente, aquellos que sean identificados como Nivel 1 por otra marca, o comercios que hayan experimentado algún compromiso de datos de tarjetas
2 1 000.000	Comercios que procesen de 1 a 6 millones de transacciones VISA anualmente	Comercios que procesen de 1 a 6 millones de transacciones MasterCard anualmente o comercios que sean calificados como Nivel 2 en otras marcas
3 200.000	Comercios que procesen 20.000 a 1 millón de transacciones VISA e-commerce anualmente	Comercios que procesen 20.000 a 1 millón de transacciones MasterCard e-commerce anualmente o comercios que sean identificados como Nivel 3 por otras marca
4	Comercios que procesen menos de 20.000 transacciones VISA e-commerce anualmente, u otros comercios que procesen hasta 1 millón de transacciones VISA anualmente	Los demás comercios que procesen MasterCard
PA-DSS - Desarrolladores de aplicaciones de pago		
Todas las empresas que comercialicen soluciones de software para pagos con tarjetas.		
Se certifica una versión específica de software		
Las marcas de tarjetas definen el requisito a los clientes de utilizar aplicaciones certificadas.		

Fuente: (CYBSEC, 2007)

Algo importante que no se debe perder de vista y que se ha mencionado previamente, es que quien exige el cumplimiento de PCI a los

establecimientos afiliados a tarjetas de crédito es la entidad bancaria (ej. VISA), y no el PCI Council, que es sólo un organismo regulador.

Para facilidad en la vigilancia y apoyo en el cumplimiento del estándar, el PCI Council creó diferentes figuras de manera que los establecimientos obtengan la ayuda adecuada de los expertos en seguridad que les orienten y evalúen el cumplimiento, detalladas a continuación:

QSA (*Qualified Security Assessor*). Este tipo de entidad es un externo que está calificado por el PCI Council para realizar evaluaciones de cumplimiento del estándar. Esta entidad a su vez atraviesa por un proceso de certificación.

ASV (*Approved Scanning Vendor*). Este tipo de entidad es un externo que está calificado para validar el apego al estándar PCI DSS realizando escaneos de vulnerabilidades de ambientes de cara a Internet, de establecimientos y proveedores de servicios (como parte del Requisito 11 del estándar).

PA-QSA (*Payment Application-Qualified Security Assessor*). El estándar PA-DSS aplica a los fabricantes de software y otros componentes que desarrollan aplicaciones que almacenen, procesen o transmitan datos del tarjeta habiente o de la tarjeta. El PA-QSA es el tipo de entidad externo que está calificado para certificar el cumplimiento del fabricante del PA-DSS (*Payment Application Data Security Standard*).

2.12.2 Requisitos de las PCI DSS

El estándar PCI DSS define 12 requerimientos básicos separados en 6 categorías y que contempla 290 controles. Los mismos abarcan todas las áreas involucradas en la seguridad del procesamiento de transacciones con tarjetas de pago (crédito o debido), y se detallan a continuación de acuerdo a PCI SSC (Council P. S., 2012):

6 CATEGORIAS:

1

Desarrollar y mantener una red segura

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas

1.1 Establezca normas de configuración para firewall y router que incluyan lo siguiente:

1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers
1.1.2 Un diagrama actualizado de la red con todas las conexiones que acceden a los datos de los titulares de tarjetas, incluida toda red inalámbrica
1.1.3 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de la red interna
1.1.4 Descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red
1.1.5 Documentación y justificación de negocio para la utilización de todos los servicios, protocolos y puertos permitidos, incluida la documentación de funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros.
Entre los servicios, protocolos o puertos no seguros se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP.
1.1.6 Requisito de la revisión de las normas del firewall y el router, al menos, cada seis meses

1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y todo componente del sistema en el entorno de los datos del titular de la tarjeta.

1.2.1 Restrinja el tráfico entrante y saliente a la cantidad que sea necesaria en el entorno de datos del titular de la tarjeta.
1.2.2 Asegure y sincronice los archivos de configuración de routers.
1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar o controlar (en caso de que ese tráfico fuera necesario para fines de negocio) todo tráfico desde el entorno inalámbrico hacia el entorno del titular de la tarjeta.

1.4 Instale 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.

1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.

1.3.1 Implemente 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 Restrinja el tráfico entrante de Internet a las direcciones IP dentro del DMZ.
1.3.3 No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.
1.3.4 No permita que las direcciones internas pasen desde Internet al DMZ
1.3.5 No permita que llegue tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta a Internet.
1.3.6 Implemente la inspección completa, también conocida como filtrado dinámico de paquetes. (Es decir, sólo se permite la entrada a la red de conexiones "establecidas").
1.3.7 Coloque 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 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

Figura 7 PCI DSS Categoría 1 Requisitos 1

6 CATEGORIAS:

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

1

Desarrollar y mantener una red segura

2.1 Siempre cambie los valores predeterminados de los proveedores antes de instalar un sistema en la red, incluidas, a modo de ejemplo, contraseñas, cadenas comunitarias de protocolo simple de administración de red (SNMP) y la eliminación de cuentas innecesarias.

2.1.1 En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transmiten datos del titular de la tarjeta, cambie los valores predeterminados proporcionados por los proveedores, incluidas, a modo de ejemplo, claves de cifrado inalámbricas predeterminadas, contraseñas y cadenas comunitarias SNMP.

2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria. Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of StandardsTechnology (NIST)

2.2.1 Implemente sólo una 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, servidores de base de datos y DNS se deben implementar en servidores separados).

2.2.2 Habilite sólo los servicios, protocolos, daemons, etc. necesarios y seguros, según lo requiera la función del sistema. Implemente funciones de seguridad para todos los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, SFTP, SSL o IPSec VPN, para proteger servicios no seguros, tales como NetBIOS, archivos

2.2.3 Configure los parámetros de seguridad del sistema para evitar el uso indebido.

2.2.4 Elimine todas las funcionalidades innecesarias, tales como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.

2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y el acceso administrativo que no sea de consola.

2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el *Anexo A: Requisitos adicionales de las PCI DSS para los proveedores de servicios de hosting compartido.*

Figura 8 PCI DSS Categoría 1 Requisitos 2

6 CATEGORIAS:

2

Proteger los datos del titular de la tarjeta

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

3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos, como se indica abajo.

3.1.1 Implemente una política de retención y disposición de datos que incluya:

- Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio
- Procesos para eliminar datos de manera cuando ya no se necesiten
- Requisitos de retención específicos para datos de titulares de tarjetas
- Un proceso automático o manual trimestral para identificar y eliminar de manera segura los datos de titulares de tarjetas almacenados que excedan los requisitos de retención definidos

3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3, establecidos a continuación:

3.2.1 No almacene contenido completo de ninguna 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 No almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes.

3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.

3.3 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).

Continua

3.4 Haga que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos:

- *Valores hash de una vía basados en criptografía sólida (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).*
- *Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas.*

3.4.1 Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Las claves de descifrado no deben estar vinculadas a cuentas de usuarios.

3.6 Documente completamente e implemente todos los procesos y los procedimientos de gestión de claves de las claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas, incluido lo siguiente:

3.6.1 Generación de claves criptográficas sólidas
3.6.2 Distribución segura de claves Criptográficas
3.6.3 Almacenamiento seguro de claves criptográficas
3.6.4 La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina 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 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción y/o revocación) según se considere necesario 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, etc.) o cuando se sospeche que las claves están en riesgo.
3.6.6 Si se utilizan operaciones manuales de gestión de claves criptográficas en texto claro, estas operaciones deben aplicar conocimiento dividido y control doble (por ejemplo, utilizando dos o tres personas, cada una de las cuales conoce su propia parte de la clave, para reconstruir toda la clave).
3.6.7 Prevención de sustitución no autorizada de claves criptográficas.
3.6.8 Requisito de que los custodios de claves criptográficas declaren formalmente que comprenden y aceptan su responsabilidad como custodios de las claves.

3.5 Proteja las claves utilizadas para asegurar los datos de los titulares de tarjeta contra divulgación o uso indebido.

3.5.1 Restrinja el acceso a las claves criptográficas al número mínimo de custodios necesarios.

3.5.2 Guarde las claves criptográficas de forma segura en la menor cantidad de ubicaciones y formas posibles.

Figura 9 PCI DSS Categoría 2 Requisitos 3.

6 CATEGORIAS:

2

Proteger los datos del titular de la tarjeta

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

4.1 Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas. Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las PCI DSS incluyen, pero sin limitarse a:

- The Internet
- Tecnologías inalámbricas
- Sistema global para comunicaciones
- móviles (GSM)
- Servicio de radio paquete general
- (GPRS)

4.1.1 Asegúrese de que las redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta utilizan las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión.

4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, el chat, etc.).

Figura 10 PCI DSS Categoría 2 Requisitos 4.

6 CATEGORIAS:

3

Mantener un programa de administración de vulnerabilidad

Requisito 5: Utilice y actualice regularmente el software o los programas antivirus

5.1 Implemente software antivirus en todos los sistemas comúnmente afectados por software malicioso (en especial, computadoras personales y servidores).

5.1.1 Asegúrese de que todos los programas antivirus son capaces de detectar y eliminar todos los tipos conocidos de software malicioso y de proteger a los sistemas contra estos.

5.2 Asegúrese de que todos los mecanismos antivirus estén actualizados, estén en funcionamiento y puedan generar registros de auditoría.

Figura 11 PCI DSS Categoría 3 Requisitos 5.

6 CATEGORIAS:

3

Mantener un programa de administración de vulnerabilidad

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

6.1 Asegúrese de que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes proporcionados por los proveedores para protección contra vulnerabilidades conocidas. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento.

6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.

6.3 Desarrolle aplicaciones de software (acceso interno y externo, e incluso acceso administrativo basado en la web a aplicaciones) de conformidad con las PCI DSS (por ejemplo, autenticación segura y registro), basadas en las mejores prácticas de la industria. Incorpore seguridad de la información en todo el ciclo de vida de desarrollo del software. Estos procesos deben incluir lo siguiente:

6.3.1 Eliminación de 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 Revisión del código personalizado antes del envío a producción o a los clientes a fin de identificar posibles vulnerabilidades de la codificación.

6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Los procesos deben incluir lo siguiente:

6.4.1 Desarrollo/prueba por separado y entornos de producción
6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo
6.4.4 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción
6.4.5 Procedimientos de control de cambios para la implementación de parches de seguridad y modificaciones del software. Los procedimientos deben incluir lo siguiente:
6.4.5.1 Documentación de incidencia.
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.
6.4.5.3 Verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.
6.4.5.4 Procedimientos de desinstalación.

Continua

6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos de alguno de los siguientes métodos:

- Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio.
- Instale un firewall de aplicación web enfrente de aplicaciones web públicas

6.5 Desarrolle aplicaciones basadas en directrices de codificación seguras. Evite vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir:

6.5.1 Errores de inyección, en especial, errores de inyección SQL. 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
6.5.3 Almacenamiento cifrado inseguro
6.5.4 Comunicaciones inseguras
6.5.5 Manejo inadecuado de errores
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).
6.5.7 Lenguaje de comandos entre distintos sitios (XSS)
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)
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF)

Figura 12 PCI DSS Categoría 3 Requisitos 6

6 CATEGORIAS:

4

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 del negocio.

7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso. Las limitaciones al acceso deben incluir lo siguiente:

7.1.1 Restricciones a los derechos de acceso a ID de usuarios privilegiadas a la menor cantidad de privilegios necesarios para cumplir con las responsabilidades del cargo
7.1.2 La asignación de privilegios se basa en la tarea del personal individual, su clasificación y función
7.1.3 Requisito de una aprobación documentada de partes autorizadas especificando privilegios requeridos.
7.1.4 Implementación de un sistema de control de acceso automático.

7.2 Establezca 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. Este sistema de control de acceso debe incluir lo siguiente:

7.2.1 Cobertura de todos los componentes del sistema
7.2.2 La asignación de privilegios a individuos se basa en la clasificación del trabajo y la función
7.2.3 Ajuste predeterminado "negar todos"

Figura 13 PCI DSS Categoría 4 Requisitos 7

6 CATEGORIAS:

4

Implementar medidas sólidas de control de acceso

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

8.1 Asigne a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a datos de titulares de tarjetas.

8.2 Además de la asignación de una ID única, emplee al menos uno de los métodos siguientes 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 Incorpore la autenticación de dos factores para el acceso remoto (acceso en el nivel de la red que se origina fuera de la red) a la red de empleados, administradores y terceros. (Por ejemplo, autenticación remota y servicio dial-in (RADIUS) con tokens; sistema de control de acceso mediante control del acceso desde terminales (TACACS) con tokens; u otras tecnologías que faciliten la autenticación de dos factores).

8.4 Deje ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante un cifrado sólido.

8.5 Asegúrese de que sean correctas la autenticación del usuario y la administración de contraseñas de usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:

8.5.1 Controle el agregado, la eliminación y la modificación de las ID de usuario, las credenciales, entre otros objetos de identificación.
8.5.2 Verifique la identidad del usuario antes de restablecer contraseñas.
8.5.3 Configure la primera contraseña en un valor único para cada usuario y cámbiela de inmediato después del primer uso.
8.5.4 Cancele de inmediato el acceso para cualquier usuario cesante.
8.5.5 Elimine/inhabilite las cuentas de usuario inactivas al menos cada 90 días.
8.5.6 Habilite las cuentas que utilicen los proveedores para el acceso remoto únicamente durante el período necesario. Supervise las cuentas de acceso remoto de proveedores cuando se utilicen.
8.5.7 Comunique los procedimientos y las políticas de autenticación a todos los usuarios con acceso a datos de titulares de tarjetas.
8.5.8 No utilice cuentas ni contraseñas de grupos, compartidas o genéricas, ni ningún otro método de autenticación.
8.5.9 Cambie las contraseñas de usuario al menos cada 90 días.
8.5.10 Solicite una longitud de contraseña mínima de siete caracteres.
8.5.11 Utilice contraseñas que contengan tanto caracteres numéricos como alfabéticos.
8.5.12 No permita que ninguna persona envíe una contraseña nueva igual a cualquiera de las últimas cuatro contraseñas utilizadas.
8.5.13 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.
8.5.14 Establezca la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.
8.5.15 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para que se active la terminal nuevamente.
8.5.16 Autentique 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. Restrinja el acceso directo a o las consultas en las bases de datos a los administradores de la base de datos.

Figura 14 PCI DSS Categoría 4 Requisitos 8

6 CATEGORIAS:

4

Implementar medidas sólidas de control de acceso

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

9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a sistemas en el entorno de datos de titulares de tarjetas.

9.1.1 Utilice cámaras de video y otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario.
9.1.2 Restrinja el acceso físico a conexiones de red de acceso público. Por ejemplo, las áreas que sean accesibles a los visitantes no deben tener puertos de red habilitados a menos que se autorice explícitamente el acceso a la red.
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones.

9.2 Desarrolle procedimientos para que el personal pueda distinguir con facilidad entre empleados y visitantes, especialmente en las áreas donde se puede acceder fácilmente a datos de titulares de tarjetas.

9.3 Asegúrese de que todos los visitantes reciban el siguiente trato:

9.3.1 Autorización previa al ingreso a áreas en las que se procesan o se conservan datos de titulares de tarjetas.
9.3.2 Token físico otorgado (por ejemplo una placa de identificación o dispositivo de acceso) con vencimiento y que identifique a los visitantes como personas no pertenecientes a la empresa.
9.3.3 Confirme que le sea solicitado entregar el token físico antes de salir de las instalaciones de la empresa o al momento del vencimiento.

9.4 Use un registro de visitas para mantener una pista de auditoría física de la actividad de visitas. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.

9.5 Almacene 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. Revise la seguridad de dicho lugar una vez al año como mínimo.

Continua

9.6 Proteja físicamente todos los medios.

9.7 Lleve un control estricto sobre la distribución interna o externa de cualquier tipo de medios que contenga datos de titulares de tarjetas, incluidos:

9.7.1 Clasifique los medios de manera que se pueda determinar la confidencialidad de los datos.
9.7.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.

9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura (especialmente cuando se los distribuye a personas).

9.9 Lleve un control estricto sobre el almacenamiento y accesibilidad de los medios.

9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.

9.10 Destruya los medios que contengan datos de titulares de tarjetas cuando ya no sea necesario para el negocio o por motivos legales, de la siguiente manera:

9.10.1 Corte en tiras, incinere o haga pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas.
9.10.2 Entregue los datos de titulares de tarjetas en dispositivos electrónicos no recuperables para que dichos datos no se puedan reconstruir.

Figura 15 PCI DSS Categoría 4 Requisitos 9

6 CATEGORIAS:

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas

5

Supervisar y evaluar las redes con regularidad

10.1 Establezca un proceso para vincular todos los accesos a componentes del sistema (especialmente el acceso con privilegios administrativos, tales como de raíz) a cada usuario en particular.

10.2 Implemente pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos:

10.2.1 Todo acceso de personas a 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 de la aplicación
10.2.7 Creación y eliminación de objetos en el nivel del sistema

10.3 Registre al menos las siguientes entradas de pistas de auditoría de 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 Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos.

10.4.1 Los sistemas críticos tienen horario uniforme y correcto.
10.4.2 Los datos de tiempo están protegidos.
10.4.3 La configuración de tiempo se recibe de fuentes aceptadas por la industria.

10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.

10.5.1 Limite la visualización de pistas de auditoría a quienes lo necesiten por motivos de trabajo.
10.5.2 Proteja los archivos de las pistas de auditoría contra las modificaciones no autorizadas.
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de inmediato en un servidor de registros central o medios que resulten difíciles de modificar.
10.5.4 Escriba registros para tecnologías que interactúen con la parte externa en un servidor de registros en la LAN interna.
10.5.5 Utilice el software de supervisión 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 Revise los registros de todos los componentes del sistema al menos una vez al día. Las revisiones de registros incluyen a los servidores que realizan funciones de seguridad, tales como sistema de detección de intrusiones (IDS) y servidores de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS).

10.7 Conserve el historial de pista de auditorías durante al menos un año, con un mínimo de tres meses inmediatamente disponible para el análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).

Figura 16 PCI DSS Categoría 5 Requisitos 10

6 CATEGORIAS:

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.

5

Supervisar y evaluar las redes con regularidad

11.1 Realice pruebas para detectar la presencia de puntos de acceso inalámbrico y de puntos de acceso inalámbrico no autorizados trimestralmente.

11.2 Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos).

11.2.1 Realice análisis de vulnerabilidad interna trimestralmente.
11.2.2 Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor Aprobado de Escaneo (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC).
11.2.3 Realice análisis internos y externos después de cualquier cambio significativo.

11.3 Realice 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). Estas pruebas de penetración deben incluir lo siguiente:

11.3.1 Pruebas de penetración de la capa de red
11.3.2 Pruebas de penetración de la capa de aplicación

11.4 Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores, líneas base y firmas de detección y prevención de intrusiones.

11.5 Implemente el software de supervisión de integridad de archivos para alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de configuración o archivos de contenido; asimismo configure el software para realizar comparaciones de archivos críticos al menos semanalmente.

Figura 17 PCI DSS Categoría 5 Requisitos 11

6 CATEGORIAS:

6

Mantener una política de seguridad de información

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

12.1 Establezca, publique, mantenga y distribuya una política de seguridad que logre lo siguiente:

12.1.1 Aborda todos los requisitos de las PCI DSS.
12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.
12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.

12.2 Desarrolle 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).

12.3 Desarrolle políticas de utilización para tecnologías críticas para empleados (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, asistentes digitales/para datos personales [PDA], utilización del correo electrónico y de Internet) para definir el uso adecuado de dichas tecnologías. Asegúrese de que estas políticas de uso requieran lo siguiente:

12.3.1 Aprobación explícita por las partes autorizadas
12.3.2 Autenticación para el uso de la Tecnología
12.3.3 Lista de todos los dispositivos y personal que tenga acceso
12.3.4 Etiquetado de dispositivos con propietario, información de contacto y objetivo
12.3.5 Usos aceptables de la tecnología
12.3.6 Ubicaciones aceptables de 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 La activación de las tecnologías de acceso remoto para proveedores y socios de negocios solo cuando es necesaria para proveedores y socios de negocios, con desactivación inmediata después del uso
12.3.10 Para que el personal tenga acceso a datos de titulares de tarjetas mediante tecnologías de acceso remoto, prohíba 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.

12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.

12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo:

12.5.1 Establezca, documente y distribuya políticas y procedimientos de seguridad.
12.5.2 Supervise y analice las alertas e información de seguridad, y distribúyalas entre el personal correspondiente.
12.5.3 Establezca, documente y distribuya los procedimientos de respuesta ante incidentes de seguridad y escalación para garantizar un manejo oportuno y efectivo de todas las situaciones.
12.5.4 Administre las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones
12.5.5 Supervise y controle todo acceso a datos.

Continua

12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.

12.6.1 Eduque al personal justo al ser contratado y, por lo menos, una vez al año.
12.6.2 Exija a los empleados que reconozcan al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa.

12.7 Examine a los empleados antes de contratarlos a fin de minimizar el riesgo de ataques desde 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).

12.8 Si los datos de titulares de tarjeta se comparten con proveedores de servicios, mantenga e implemente políticas y procedimientos a los fines de que los proveedores de servicio incluyan lo siguiente:

12.8.1 Mantenga una lista de proveedores de servicios.
12.8.2 Mantenga 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 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.
12.8.4 Mantenga un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios.

12.9 Implemente un plan de respuesta a incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.

12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente:

- 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 Pruebe el plan al menos una vez al año.
12.9.3 Designe personal especializado que se encuentre disponible permanentemente (24/7) para responder a las alertas.
12.9.4 Proporcione capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad.
12.9.5 Incluya alertas de sistemas de detección y prevención de intrusiones, y de supervisión de integridad de archivos.
12.9.6 Elabore un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria.

Figura 18 PCI DSS Categoría 6 Requisitos 12

2.13 PCI DSS vs ISO 27001

La norma ISO/IEC 27001:2005[7] define los requerimientos para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI (Sistema de Gestión de Seguridad de la Información). Es una norma certificable que se ha convertido en el estándar internacional en gestión de seguridad de la información. La figura 7 enmarca todos los ámbitos de ISO 27001

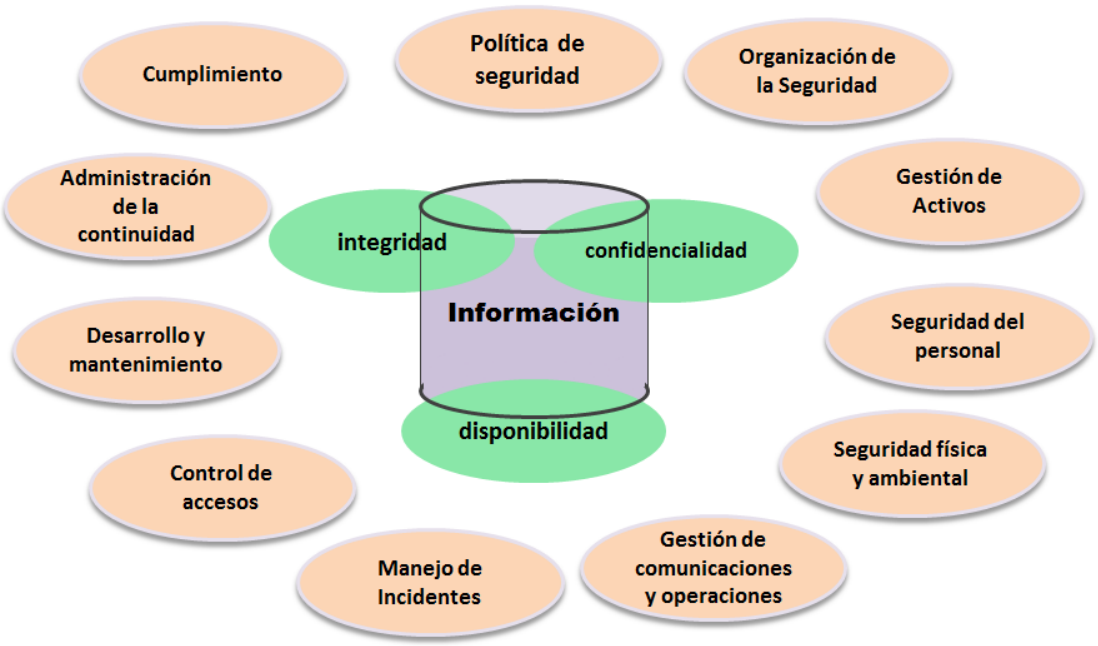


Figura 19 Ámbitos de ISO27001

Fuente: (Normativa ISO 2700)

Uno de los aspectos que remarca ISO27001 en su cláusula 4.2.1) b) 2) es que se deben tener en cuenta los requerimientos legales, regulatorios, de negocio y contractuales que deben ser cumplidos, por lo que podríamos encajar PCI DSS como uno de los requerimientos a cumplir como parte del SGSI que opera en la organización.

[7] Por sus siglas en inglés: International Organization for Standardization/International Electrotechnical Commission (Organización Internacional para la Normalización/ Comisión Electrotécnica Internacional)

Por otro lado, ISO27001 exige que las medidas de seguridad que se implanten estén justificadas en base al riesgo que soporta la organización y en base al riesgo aceptable para ésta, de manera que como resultado del análisis de riesgos se decidirán aquellos riesgos que se quieren gestionar y se determinarán los controles a implementar tomando como base los del Anexo A (ISO17799), aunque pueden utilizarse otros si se considera conveniente. Los objetivos de control que PCI DSS establece son de obligado cumplimiento y lo único que podemos hacer es utilizar controles compensatorios en caso de no poder cumplir un objetivo de control tal y como se especifica. La tabla 2, muestra la relación entre los controles de ISO 27001 y los requisitos de PCI DSS.

Tabla 2

Relación de controles ISO27001 y requisitos PCI DSS

PCI DSS	ISO 27001 (ANEXO A)										
	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
1		X				X	X				X
2							X	X			
3						X	X	X			X
4								X			
5						X	X				
6						X	X	X			X
7							X				
8							X				
9			X		X	X	X				
10						X					X
11						X	X	X			X
12	X	X	X	X		X	X	X	X	X	

Fuente: (Normativa ISO 2700)

Aunque ISO27001 cubre los requerimientos PCI DSS, en algunos casos faltan detalles de implementación (granularidad) que PCI DSS sí lo específica. Por tanto, puede utilizarse ISO27001 para gestionar el cumplimiento de PCI DSS, pero a la hora de implementar este cumplimiento se deberá analizar y seguir exactamente lo que PCI DSS especifica que debe hacerse para cumplir cada requerimiento. La tabla 3, muestra una comparación de las características:

Tabla 3

Características PCI DSS e ISO 27001

CARACTERISTICA	PCI DSS	ISO 27001
Implementación de controles	Mandatorio	Basado en la evaluación de riesgo
Granularidad (*)	Alta	Baja
Grado de flexibilidad	Baja	Alta
Gestión	Baja contribución	Alta contribución

Fuente: (Normativa ISO 2700)

(*) La granularidad se refiere a que se especifica un nivel de detalle en el cual se identifica todos los componentes del estándar (información altamente o mínimamente detallada). Una alternativa podría ser definir el SGSI con un ámbito muy específico, y que sería el que afecta a la transmisión, almacenamiento y procesamiento de datos de tarjetas de pago, el ámbito de PCI DSS. El objetivo de hacer esto sería obtener la certificación ISO27001 dentro de este alcance concreto y aprovechar el trabajo realizado para cumplir PCI DSS como base para reducir el tiempo y coste necesario de implantar ISO27001.

Modelo de factibilidad para el cumplimiento de normas de seguridad de datos en tarjetas de pago alineados al estándar PCI DSS para las entidades bancarias de Ecuador.

CAPITULO III

ANALISIS DE SITUACION ACTUAL

"La imaginación es más importante que el conocimiento. El conocimiento es limitado, mientras que la imaginación no"

— Albert Einstein

CAPÍTULO III

ANALISIS DE SITUACION ACTUAL

3.1 Antecedentes

En los últimos años Internet ha pasado de ser una herramienta prioritaria a convertirse en un fenómeno social y de uso masivo inclusive considerando dentro de los servicios básicos.

Sin embargo el crecimiento de usuarios que acceden al servicio de Internet crece exponencialmente lo cual podemos evidenciarlo en el estudio histórico realizado por Internet y se presenta en la figura 20:

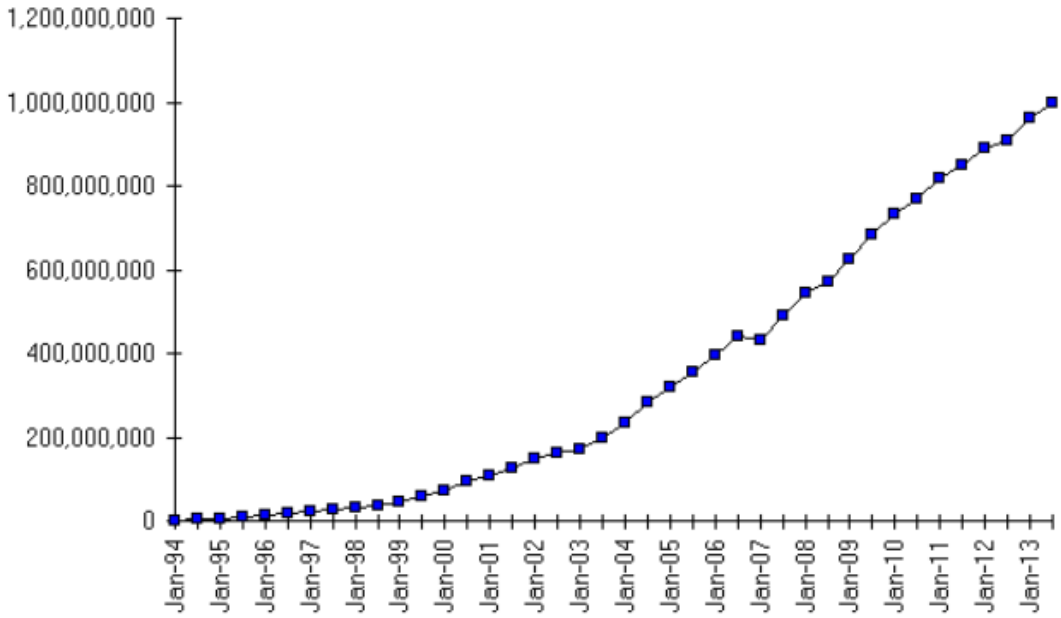


Figura 20 Encuesta número de usuarios de Internet anual

Fuente: (INEC, 2012)

En el curso de los últimos seis años el número de usuarios de Internet se ha duplicado, y actualmente hay más de dos mil millones de usuarios de Internet en todo el mundo. Las tasas de crecimiento fue mayor en los países

en desarrollo con el 16% que en los países desarrollados con el 5% existiendo una gran diferencia en los porcentajes de penetración de internet, así a finales del 2011 el 70% corresponde a los países desarrollados en comparación con el 24% en los países en desarrollo. Con respecto al total mundial de usuarios de internet en los países en desarrollo ha aumentado del 44% en el 2006 al 62% en el 2011. A finales del 2011 el 32.5 % de la población mundial estaba en línea, esto es claramente evidenciado en la información de la base de datos de la UIT sobre indicadores mundiales de las Telecomunicaciones presentado en la figura 21:

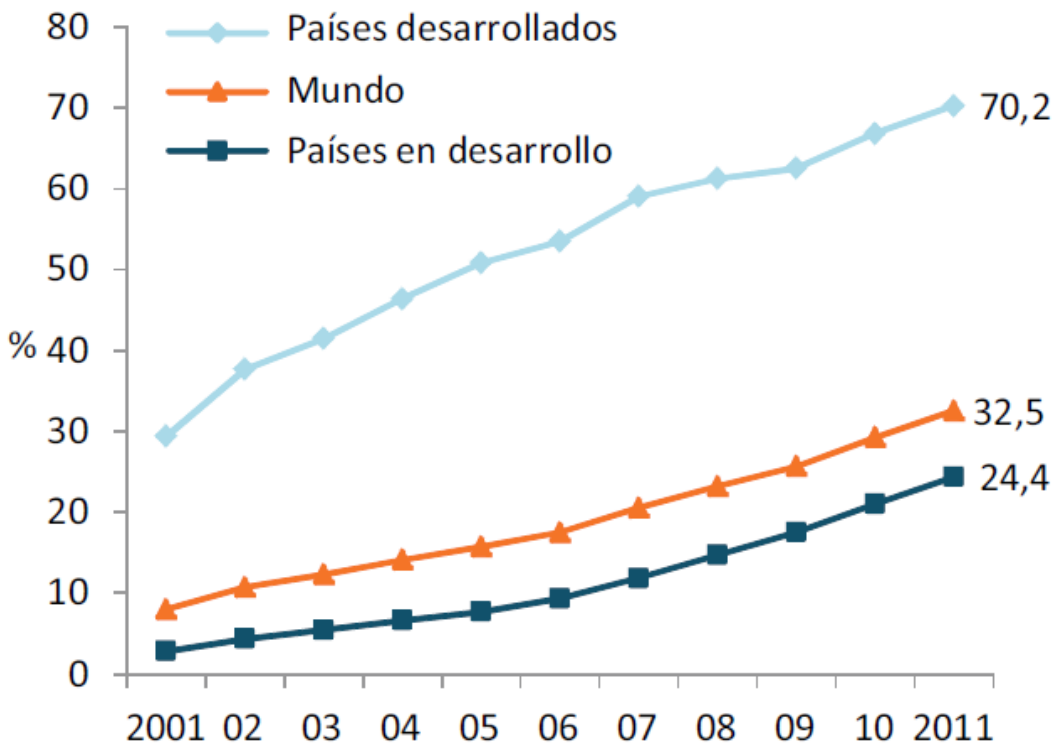


Figura 21 Usuarios de Internet en el mundo y por nivel de desarrollo, 2001-2011

Fuente: (ITU, 2012)

En Ecuador el crecimiento del acceso al servicio de internet, al igual que la línea mundial continua incrementándose de manera exponencial, en la figura 22 podemos observar estadísticas hasta el 2010 de tres fuentes distintas:

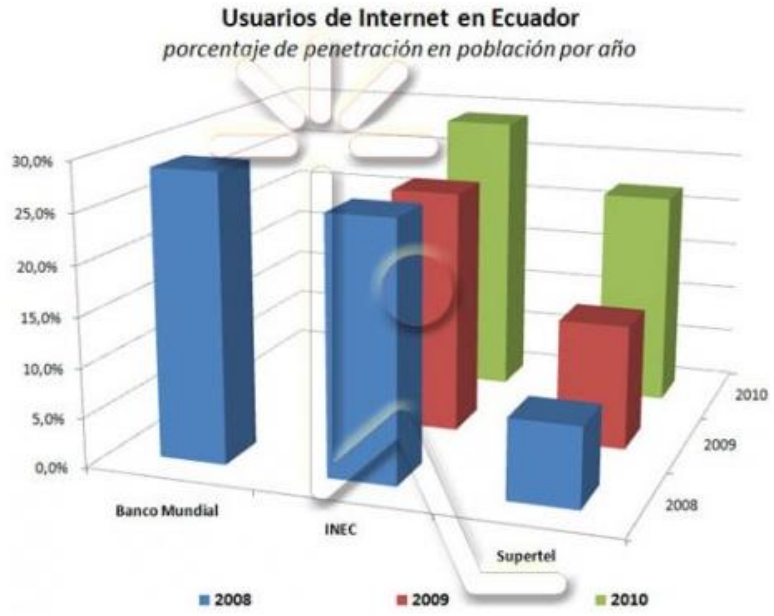


Figura 22 Usuarios de Internet en Ecuador comparativa varias fuentes

Fuente: (ITU, 2012)

En las figuras 23 y 24 se presentan otras estadísticas comparativas de los últimos años acotando el crecimiento que relacionado con el número total de habitantes 14.483.499 habitantes al 2011 se tiene cerca de un 45 % de la población con acceso a internet.

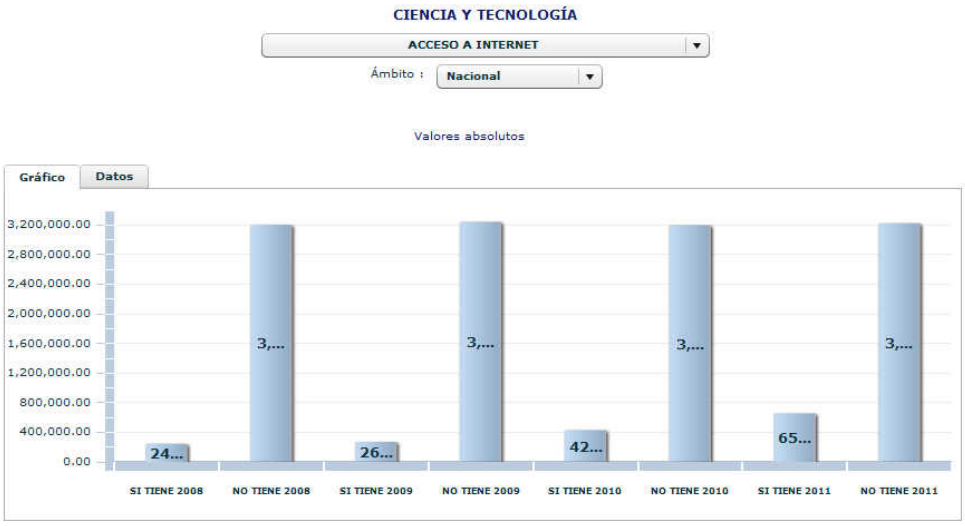


Figura 23 Usuarios con acceso a internet a nivel nacional

Fuente: (INEC, 2012)

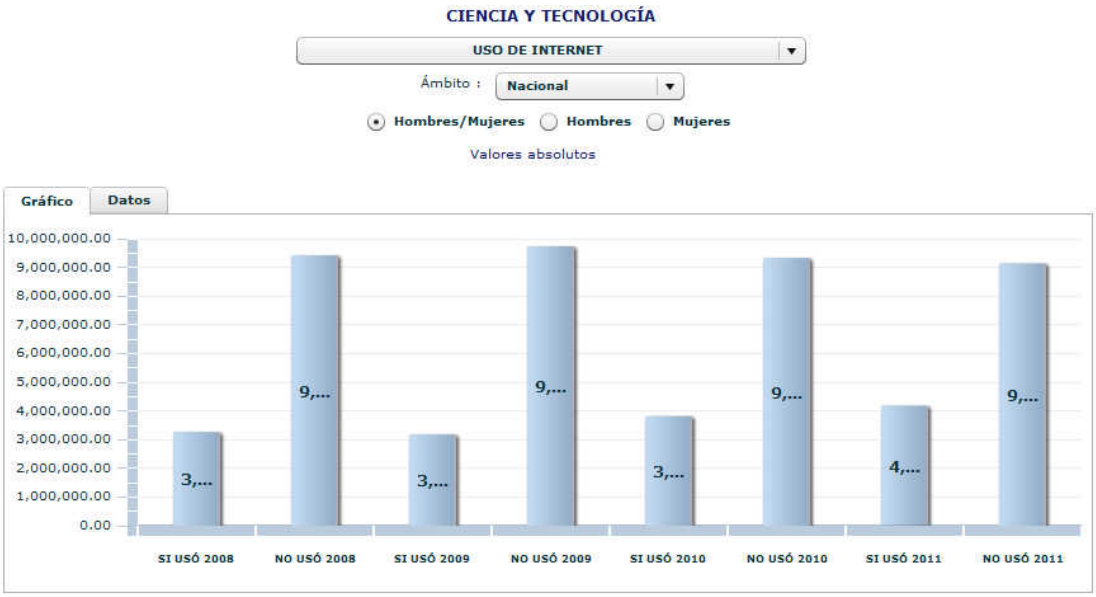


Figura 24 Uso de internet a nivel nacional

Fuente: (INEC, 2012)

La figura 25 muestra una comparación de los porcentajes de usuarios con acceso a Internet a nivel de los países sudamericanos en la cual se puede evidenciar la tendencia al crecimiento.

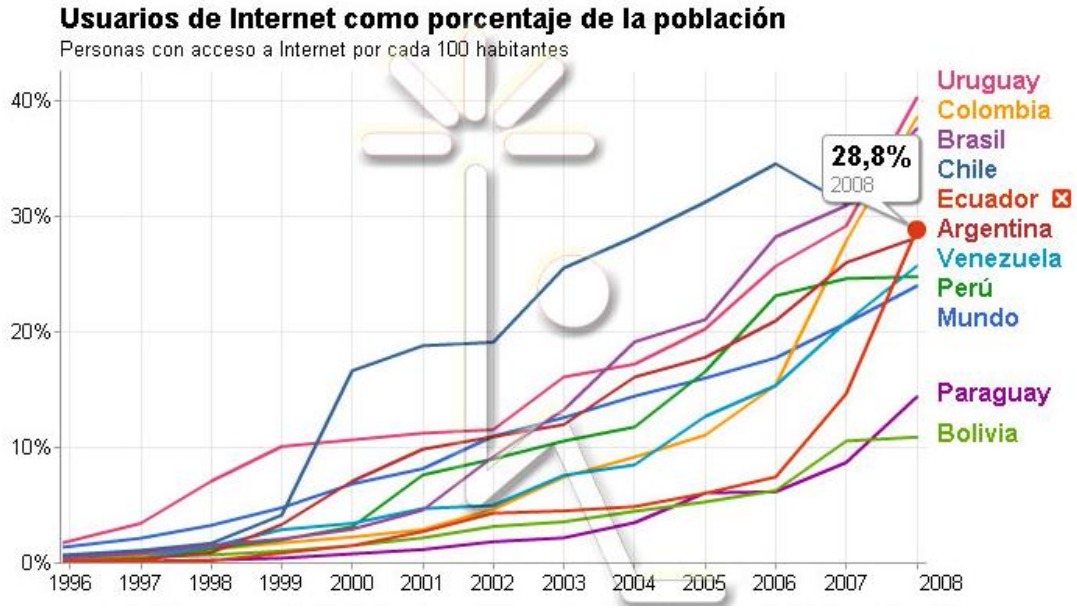


Figura 25 Uso de internet en Sudamérica

Fuente: (INEC, 2012)

Esta masificación del servicio y los beneficios que ofrecen las nuevas tecnologías viene acompañada de eventos que atentan contra la seguridad de los datos y en caso del uso del Internet en transacciones bancarias se torna crítico por el perjuicio económico que puede causar (al usuario y a la entidad bancaria). Al usuario le preocupa mucho el fraude y no creen que la seguridad en Internet este mejorando, pero no conocen los tipos de amenazas que los pueden afectar. Al no conocer las amenazas no se protegen contra estas y generalmente al sufrir un fraude o como medida de prevención dejan de hacer transacciones bancarias por Internet o cambian de banco.

Piensan que el mayor responsable de su protección es el banco, antes que los usuarios. Creen que los bancos deben implementar métodos adicionales de seguridad, lo que aumentaría en forma importante su percepción de seguridad y esperan que monitoreen sus transacciones para detectar acciones sospechosas. Están dispuestos a usar medidas adicionales de seguridad pero no a pagar por servicios adicionales mismos que deben ser regulados por el ente de control que en nuestro país la responsabilidad recae sobre la SUPERINTENDENCIA DE BANCOS Y SEGUROS (SBS).

Las entidades bancarias deben tomar medidas adicionales de seguridad, mismas que deben venir acompañadas de educación para incrementar la confianza, evitar pérdida de clientes e incrementar la base de usuarios y la frecuencia de uso de Internet y otros canales menos costosos que las oficinas. La lucha contra el fraude electrónico se lo debe considerar como crítico dado que mientras más bajo sea el porcentaje de su presencia evitará pérdidas económicas y mantendrá la confianza y credibilidad a las entidades bancarias y fundamentalmente incentivar al crecimiento de la banca online y de nuevos canales electrónicos.

3.2 Superintendencia de Bancos y Seguros

3.2.1 Reseña Histórica

A partir de 1830 tras la independencia de Ecuador se manejaba una economía poco monetizada con circulación de oro y plata, y caracterizado por ser agrícola y comercial con actividades orientadas al comercio exterior se enfrentó una insuficiencia de recursos monetarios.

En 1832 se dicta por primera vez una Ley de Monedas en la República del Ecuador, regulando la exportación de monedas, emisiones particulares y falsificaciones.

En 1869 se promulgó la Ley de Bancos Hipotecarios, cuya vigilancia, a pesar de ser incompleta, se mantuvo durante más de cincuenta años, y en 1899 y se elabora la Ley de Bancos regulando 6 entidades dedicadas a la fabricación de monedas y manejo de negocios bancarios.

En 1914 se nombra por primera vez una autoridad de supervisión de los bancos en el cargo de Comisario Fiscal de Bancos encargado de vigilar la emisión y cancelación de los billetes de bancos; hasta que en 1927 se produjo una verdadera transformación en el ámbito bancario y financiero al expedir la Ley Orgánica de Bancos, la Ley Orgánica del Banco Hipotecario (Banco Nacional de Fomento) y la Ley Orgánica del Banco Central con las cuales se afianzaron el sistema financiero del país.

Es así como a partir del 6 de septiembre de 1927 se crea la Superintendencia de Bancos y Seguros (SBS) (SuperIntendencia de Bancos y Seguros, 2012)

3.2.2 Generalidades de la Superintendencia de Bancos y Seguros.

3.2.2.1Objetivos Institucionales

Los objetivos institucionales publicados por la SBS son (SuperIntendencia de Bancos y Seguros, 2012):

- Fortalecer el marco legal y normativo de acuerdo a principios, mejores prácticas y estándares internacionales vigentes.
- Lograr una adecuada administración de riesgos mediante el fortalecimiento de los procesos de supervisión de los sistemas controlados.
- Proteger los derechos de los consumidores financieros.
- Fortalecer la gestión organizacional y la administración del recurso humano.
- Asegurar la calidad y la seguridad de la información y el servicio informático, con tecnología de punta.
- Optimizar la administración de los recursos financieros

3.2.2.2Visión

Ser un organismo autónomo e independiente de regulación y supervisión, que ejerza su mandato constitucional y legal según las mejores prácticas internacionales, que consolide la confianza de la sociedad, coadyuvando a la sostenibilidad de los sistemas controlados y a la protección del usuario; apoyado en capital humano competente y con recursos materiales y tecnológicos adecuados. (SuperIntendencia de Bancos y Seguros, 2012)

3.2.2.3Misión

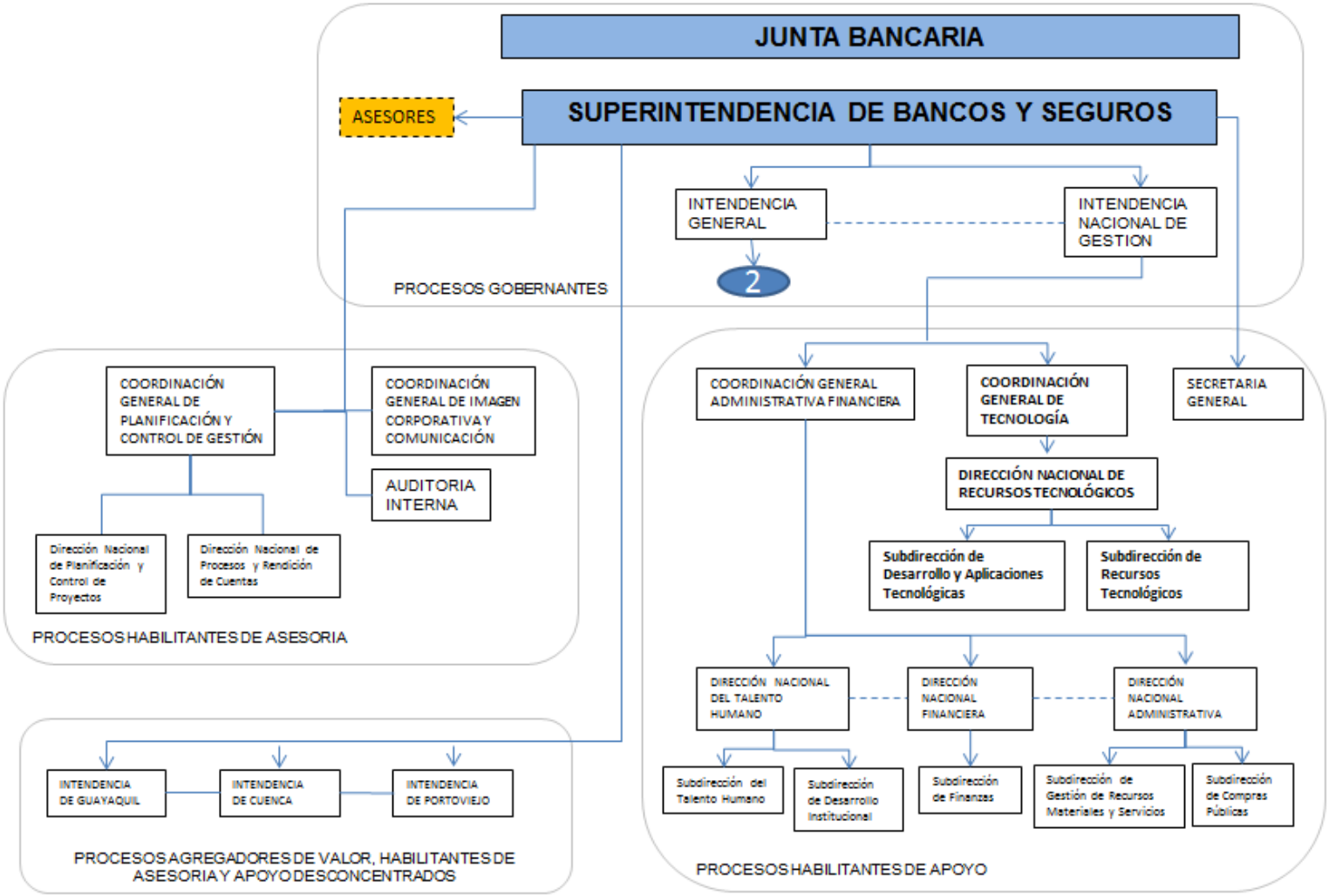
Velar por la seguridad, estabilidad, transparencia y solidez de los sistemas financiero, de seguros privados y de seguridad social, mediante un eficiente y eficaz proceso de regulación y supervisión para proteger los intereses del

público e impulsar el desarrollo del país. (SuperIntendencia de Bancos y Seguros, 2012)

3.2.3Organigrama de la SBS

De acuerdo al Capítulo I, Articulo1 de RESOLUCIÓN N° ADM-2012-10779 6 DE FEBRERO DE 2012, la Superintendencia de Bancos y Seguros, para garantizar el cabal cumplimiento de su misión, responsabilidades y objetivos, está integrada por las siguientes unidades detalladas en la figura 26 (SuperIntendencia de Bancos y Seguros, 2012):

ORGANIGRAMA DE POSICION DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS



Continua

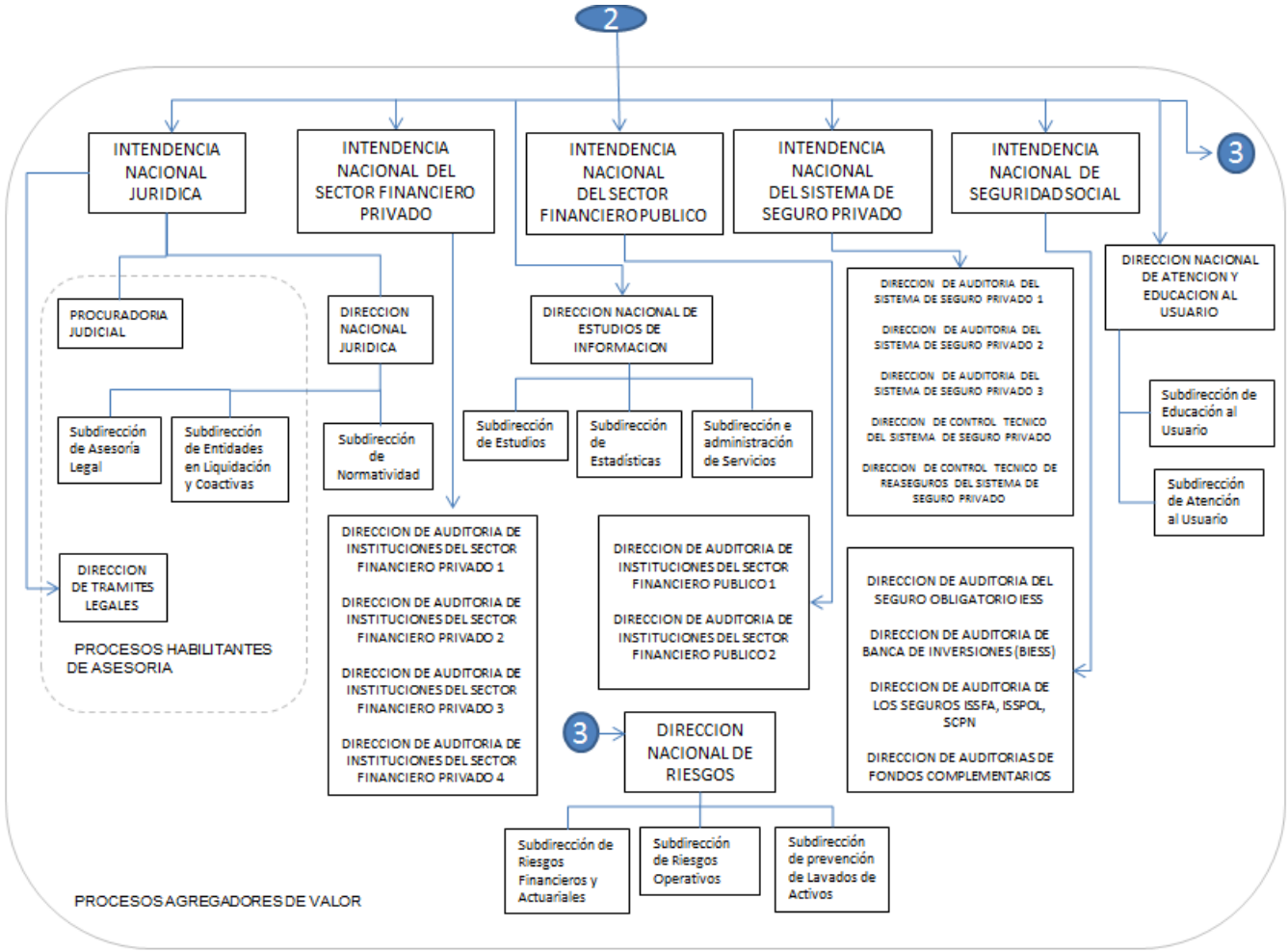


Figura 26 Organigrama SBS

Fuente: (SuperIntendencia de Bancos y Seguros, 2012)

3.2.4Entidades Bancarias del Ecuador suscritas a la SBS

Las entidades bancarias privadas de Ecuador actualmente activas y suscritas a la SBS son las detalladas a continuación (SuperIntendencia de Bancos y Seguros, 2012):

Tabla 4

Bancos Privados Nacionales activos

Código Institución	Nombre Institución	Ultimo Estado	Fecha de Resolución	Resolución
1002	BP AMAZONAS	ACTIVA	1975/07/10	SB-75-438
1004	BP AUSTRO	ACTIVA	1977/07/27	77-386
1007	BP BOLIVARIANO	ACTIVA	1979/04/04	SB-79-235
1151	BP CAPITAL	ACTIVA	2007/06/07	SBS-INIF-2007-450
1010	BP COFIEC	ACTIVA	1995/03/07	SB-95-1922
1011	BP COMERCIAL DE MANABI	ACTIVA	1979/07/10	SB-79-285
1134	BP COOPNACIONAL	ACTIVA	1985/10/28	SB-85-076
3960	BP D-MIRO S.A.	ACTIVA	2010/11/24	SBS-2010-844
1422	BP DELBANK	ACTIVA	2003/11/10	222
1165	BP FINCA	ACTIVA	2007/08/14	SBS-2007-0701
1020	BP GENERAL RUMIÑAHUI	ACTIVA	1988/07/14	SB-88-1350
1006	BP GUAYAQUIL	ACTIVA	1996/07/31	SB-96-0407
1023	BP INTERNACIONAL	ACTIVA	1973/09/04	SB-73-709
1014	BP LITORAL	ACTIVA	1988/07/11	SB-88-1347
1025	BP LOJA	ACTIVA	1968/02/05	SB-68-212
1026	BP MACHALA	ACTIVA	1962/06/20	SB-62-307
1028	BP PACIFICO	ACTIVA	1972/01/18	SB-72-286
1029	BP PICHINCHA	ACTIVA	1906/04/02	FUNDACION
1148	BP PROCREDIT	ACTIVA	2004/09/23	SBS-2004-0753
1033	BP PRODUBANCO	ACTIVA	1978/03/27	SB-78-45
1418	BP PROMERICA	ACTIVA	2009/02/03	SBS-2009-0135
1037	BP SOLIDARIO	ACTIVA	1996/07/29	SB-96-395
1038	BP SUDAMERICANO	ACTIVA	1994/10/06	SB-94-1587-
1039	BP TERRITORIAL	ACTIVA	1936/11/26	SB-36-284
1041	BP UNIBANCO	ACTIVA	1964/11/16	DECRETO 2639

Fuente: (SuperIntendencia de Bancos y Seguros, 2012)

Las entidades bancarias públicas son:

Tabla 5

Instituciones Bancarias Públicas

Código Institución	Nombre Institución	Ultimo Estado	Fecha de Resolución	Resolución
1051	BANCO DEL ESTADO	ACTIVA	1976/09/17	SB-76-D774
1050	BCE	ACTIVA	1927/03/12	SB-27-D283
1052	BEV	ACTIVA	1961/05/26	SB-61-D223
3927	BIESS	ACTIVA	2009/05/11	LEY DEL BIESS
1053	BNF	ACTIVA	1964/11/24	DEC. SUPREMO 2767
1054	CFN	ACTIVA	1964/08/21	R.O. 316
3808	FODEPI	ACTIVA	2007/09/21	R.O. 175
1056	IECE	ACTIVA	1971/04/26	SB-71-S601

Fuente: (SuperIntendencia de Bancos y Seguros, 2012)

3.3 Regulación Ecuatoriana Ajustada a los Requerimientos de PCI DSS

El Comité de Basilea emitió el documento Basilea II en el año 2003, el cual contiene los Principios sobre la Gestión del Riesgo Operativo, para su implementación en las entidades bancarias. La Junta Bancaria a través de la Resolución No. JB-2005-834 de octubre-2005, emitió la norma sobre la "Gestión del Riesgo Operativo": **LIBRO I.-** NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO; **TITULO X.-** DE LA GESTION Y ADMINISTRACION DE RIESGOS; **CAPÍTULO V.-** DE LA GESTIÓN DEL RIESGO OPERATIVO.

De manera general la norma considera:

- Los principios del Comité de Basilea;

- Los aspectos relevantes de la literatura de la “Administración de Procesos” y de la “Administración del Recurso Humano”;
- El “Código de práctica para la administración de la Seguridad de la Información”, contenidas en la norma ISO 27002 (ISO 17799);
- Las mejores prácticas para TI establecidas por el Modelo CobiT.

La Norma de Riesgo Operativo es el resultado de la situación real del sistema financiero del 2005 y las prácticas de riesgo operativo emitidas por el Comité de Basilea, y debe estar implementada en las entidades financieras para contribuir con la seguridad de los intereses del cliente y la solidez del Sistema Financiero del Ecuador, esta norma es exigida y supervisada por la SBS en las entidades financieras.

3.3.1 El Riesgo Operativo en Ecuador

De acuerdo a la norma del LIBRO I.- NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO, TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; en su Artículo 3, define el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos (Superintendencia de Bancos y Seguros, 2005).

En la sección II, articulo 4, numeral 4.3 menciona que “Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.” (SBS, 2012)

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información. Dichas políticas, procesos y procedimientos se referirán a: Planificación estratégica, Administración de las aplicaciones, Operaciones de tecnología, Servicios de TI provistos por terceros, administración de la infraestructura tecnológica, y seguridad de la información.

3.3.2 SBS y la Seguridad en Canales Electrónicos

La Superintendencia de Bancos y Seguros del Ecuador ha trabajado en el desarrollo de disposiciones normativas para exigir a las instituciones financieras controladas, la implementación de medidas de seguridad en sus canales electrónicos. Estas disposiciones forman parte complementaria de la norma de Gestión del Riesgo Operativo, y permitirán aportar de manera importante en la mitigación de los riesgos de fraude interno y externo que en los últimos años se ha presentado recurrentemente en el Ecuador en cuanto a la clonación de la banda magnética de las tarjetas de crédito, cajero automático y débito, así como el robo de fondos de los clientes mediante la técnica del Phishing a través de Internet.

A partir del abril del 2012, se publica la RESOLUCION JB-2012-2148 con cambios principalmente en el título X “De la gestión integral y control de riesgos”, del citado libro I, consta el capítulo V “De la gestión del riesgo operativo”; en los cuales las entidades financieras se han enfocado dado los plazos de cumplimiento que la SBS ha establecido.

Principalmente, las disposiciones normativas hacen referencia a (SBS, 2012):

- La colocación de dispositivos para prevenir y alertar sobre la colocación de lectoras falsas de tarjetas en los cajeros automáticos, así como de

cerraduras para fortalecer las seguridades de acceso físico a su interior.

- La adopción de estándares de seguridad que estén difundidos a nivel mundial para el uso y manejo de canales electrónicos, razón principal de la propuesta presentada en este documento, entre las que están la transferencia segura de información confidencial abarcada en el estándar PCI DSS.
- La implementación de mecanismos para que los clientes personalicen las condiciones en sus transacciones mediante canales electrónicos e instrumentos para realizar operaciones, así como su bloqueo en caso de eventos inusuales que adviertan situaciones fraudulentas; y el registro del perfil de los clientes sobre sus costumbres transaccionales. Como ejemplo de este mecanismo se encuentra el Sistema Biométrico implementado en Banco Pichincha a finales del 2011, el cual consiste en un conjunto de preguntas y respuestas que el usuario define en función de su perfil y datos personales e incluso basados en la velocidad de digitación de los datos requeridos.
- Las entidades deberán enviar mensajes en línea sobre la confirmación de acceso y/o ejecución de transacciones mediante canales electrónicos e instrumentos para realizar operaciones. También deberán realizar como mínimo una vez al año y en caso de cambios, una prueba de vulnerabilidad y penetración a la infraestructura tecnológica usada para los canales electrónicos.
- Las instituciones financieras deben implementar microprocesador o chip (tarjetas inteligentes) en los instrumentos para realizar operaciones, y los cajeros automáticos y POS deberán ser capaces de procesar la información de las tarjetas inteligentes.
- También deberán mantener permanentemente informados a los clientes sobre los riesgos derivados del uso de canales electrónicos y de los instrumentos para realizar operaciones, así como sobre las

medidas de seguridad a tener en cuenta al efectuar transacciones mediante canales electrónicos y con medios de pago.

- Además, para que los establecimientos comerciales procesen en presencia del cliente las transacciones, los POS o PIN PAD deben permitir las comunicaciones inalámbricas de manera segura.

- Por otro lado, también deberán implementar mecanismos de control, autenticación y monitoreo para reducir la posibilidad de que los clientes sean engañados y accedan a páginas falsas similares a las propias de las instituciones financieras. Así como establecer un tiempo máximo de inactividad después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación para realizar otras transacciones.

- Adicionalmente, las entidades deberán implementar mecanismos de autenticación al inicio de sesión en donde el nombre de usuario debe ser distinto al número de cédula y debe combinar caracteres numéricos y alfanuméricos. Y en la ejecución de transacciones, deberán implementar autenticación fuerte.

3.3.3 Análisis de la Normativa de la SBS y el Estándar PCI DSS.

Al analizar el Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo podemos indicar que en dicha norma se encuentran definidas las seis categorías con sus requisitos exigidas por PCI DSS; en la Tabla 6 se muestra dicha comparación así como la revisión de los requisitos aun no contemplados y la perspectiva de donde deben ser definidas:

Tabla 6

Análisis de normativa SBS y PCI DSS

<table>
<tr><th colspan="2" rowspan="2">CONTROLES PCI</th><th colspan="2">NORMATIVA DE LA SUPERINTENDENCIA DE BANCOS Y SEGUROS</th></tr>
<tr><th colspan="2">Disposiciones normativas</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Desarrollar y mantener una red segura</td><td colspan="2">Las entidades deben tener controles para asegurar la integridad, disponibilidad y confidencialidad de la información bajo su gestión; Quienes ofrezcan servicio de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro mediante técnicas de encriptación; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.</td></tr>
<tr><td>Ubicación de la norma</td><td>Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo</td></tr>
<tr><td colspan="2">Deben estar implementados sistemas de control y autenticación para evitar accesos no autorizados y ataques externos.</td></tr>
<tr><td>Ubicación de la norma</td><td>Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="4">2</td><td rowspan="4">Proteger los datos del titular de la tarjeta</td><td colspan="2">Controles para impedir acceso indebido a consultar información confidencial de los clientes en ambiente de producción. Aquella información confidencial en ambientes de desarrollo y pruebas debe ser enmascarada o codificada.</td></tr>
<tr><td>Ubicación de la norma</td><td>SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS</td></tr>
<tr><td colspan="2">Quienes ofrezcan servicio de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro mediante técnicas de encriptación; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.</td></tr>
<tr><td colspan="2"></td></tr>
</table>

Continua

		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		La transmisión de información confidencial de clientes (incluyendo tarjetas) vía Internet debe ser encriptado.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Se debe contar con protocolos seguros y certificados digitales en las páginas web de las entidades, e incluir el uso de técnicas de encriptación de los datos transmitidos.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Contar con mecanismos de seguridad que impidan que la información de las transacciones de los clientes sea capturada por terceros no autorizados.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
3	**Mantener un programa de administración de vulnerabilidad**	Existencia de controles para detectar y evitar la instalación de software no autorizado o sin licencia, y la instalación / actualización periódica de sistemas para detección y desinfección de virus y software malicioso.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		Contar en sus cajeros automáticos con software antimalware que permita proteger el software instalado, detectar intentos o alteraciones en su código, configuración y/o funcionalidad. Y emitir alarmas para su bloqueo, inactivación y posterior revisión técnica.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Controles para asegurar la integridad, disponibilidad y confidencialidad de la información administrada; metodologías formales para que el desarrollo y mantenimiento de aplicaciones sea seguro y bajo estándares, y procedimientos para la administración y control de compra de software; todo ello con la aceptación de los usuarios involucrados. Controles para una segura administración de versiones. Definición de responsables de la información, quienes deben definir y autorizar de forma controlada los accesos y cambios funcionales en las aplicaciones, así como monitorear el cumplimiento de los controles implementados.	

Continua

		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
4	**Implementar medidas sólidas de control de acceso**	Controles para impedir accesos indebidos a consultar información confidencial de los clientes en ambiente de producción. Aquella confidencial en ambientes de desarrollo y pruebas debe ser enmascarada o codificada.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Sistemas de administración de las seguridades de acceso a la información, definiendo las facultades y atributos de los usuarios, en el registro, eliminación y modificación de datos, y pistas de auditoría, en todos los ambientes de procesamiento. Niveles de autorización de accesos para la ejecución de funciones en las aplicaciones, con segregación de funciones. Implementados sistemas de control y autenticación para evitar accesos no autorizados y ataques externos.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		Medidas de seguridad física sobre cajeros automáticos, principalmente: protectores de teclado y del lector de tarjetas, iluminación, vigilancia, anclaje, controles de acceso al sistema operativo, cámaras y grabación de imágenes.	
		Ubicación de la norma	*Libro I, Título II, Capítulo I: Apertura y cierre de oficinas*
		Controles para proteger la información de documentos o de medios de almacenamiento interno o externo, en su uso y transmisión, contra daño, robo, acceso no autorizado, utilización o divulgación indebida. Instalaciones de procesamiento protegidas con controles que impidan el acceso de personal no autorizado para evitar daños en los equipos y en la información.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativ o*

Continua

5	**Supervisar y evaluar las redes con regularidad**	Contar con políticas y procedimientos que permitan una adecuada administración, monitoreo y documentación de las bases de datos, redes, software base y hardware.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		Mecanismos de monitoreo y control que emitan alarmas para notificar sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Monitoreo periódico sobre la efectividad de las seguridades del hardware, software, redes y comunicaciones, y sobre cualquier otro elemento o dispositivo utilizado en canales electrónicos. Mantener registros históricos de las operaciones realizadas a través de éstos. Realizar pruebas periódicas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones; y definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.	
		Ubicación de la norma	*SE DEBE DEFINIR EN FUNCION DE LA SEGURIDAD EN CANALES ELECTRONICOS*
		Monitorear el desempeño del sistema de administración de la seguridad de la información para tomar acciones para mejorarlo continuamente.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
6	**Mantener una política de seguridad de información**	Contar con políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, y las consecuencias de violación de estas políticas.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*

Continua

		Identificar los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente la evaluación de los riesgos existentes, los requisitos legales, normativos, reglamentarios y contractuales, y los principios, objetivos y condiciones necesarios para procesar la información que respalda las operaciones del negocio.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		Clasificar y controlar los activos de TI, considerando su registro, identificación, y los responsables de su uso y mantenimiento.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*
		Definir los responsables (propietarios) de la información, quienes deben establecer y autorizar de forma controlada, los accesos y los cambios funcionales en las aplicaciones, así como monitorear el cumplimiento de los controles implementados.	
		Ubicación de la norma	*Libro I, Título X, Capítulo V: Gestión del Riesgo Operativo*

Fuente: (SuperIntendencia de Bancos y Seguros, 2012)

3.3.4 Encuesta al Departamento Tecnológico de la Infraestructura Actual

A fin de conocer el estado actual de las entidades bancarias respecto al nivel de cumplimiento de los requerimientos de PCI DSS, se presenta un formato de encuesta la misma que nos dará una idea de conocer las actividades a ejecutar en la plataforma o infraestructura tecnológica de determinada entidad encaminada a alcanzar la certificación PCI DSS.

El formato pueden responderlo el Gerente IT, Responsable del Departamento de Tecnología, Administrador de red, Administrador de Seguridades. En la primera fase solo se requiere una breve respuesta SI o NO a través de la cual podemos evaluar las necesidades a cumplir, el esfuerzo requerido y poder presentar una propuesta de solución y su factibilidad de ejecución en función de los costos implicados.

3.3.4.1 Formato de Encuesta

En la Tabla 7, se presenta el formato propuesto, en la cual se detalla una serie de preguntas comprensivas y estructuradas en función de los requisitos a cumplir en el estándar PCI DSS, se propone el área responsable quien debe contestar cada pregunta y la respuesta es de selección entre 4 alternativas referentes al porcentaje de cumplimiento de cada ítem; adicional se encuentra la opción de identificar la causa por la cual no se cumple con el requerimiento al 100%. Dicha información ayudará a identificar las falencias a nivel tecnológico en cada uno de los aspectos que intervienen.

El formato puede ser ajustado al organigrama de administración tecnológica definido en cada entidad bancaria, considerando como mínimo que se contemple un Gerente IT, departamento de Seguridad y Riesgo de la información, Administrador de redes, Administradores de servidores e infraestructura ; departamento de soporte al usuario y un departamento de recursos humanos.

Tabla 7

Formato de Encuesta a personal de IT

INFORMACION GENERAL PARA DEFINIR NIVEL DE CUMPLIMIENTO ESTANDAR PCI DSS			
Políticas, Normas, Estándares y Procedimientos de los Componentes del Sistema			
Ítem	**AREA RESPONSABLE**	**Proceso / Documentos/ Política**	**% Cumplimiento**
Red Segura		**Equipos Seguridad Perimetral**	
1	Seguridad y Riesgo de la información	o Requerimientos para implementar Firewall en cada conexión de Internet y entre cualquier DMZ o zona segura y la intranet	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
2	Seguridad y Riesgo de la información	o Procedimiento y control de instalaciones bajo gestión de proveedores	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	**Seguridad y Riesgo de la información**	**o Procedimiento accesos aplicaciones PCI y control ubicación zona especifica**	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Seguridad y Riesgo de la información	o Procedimiento de ABM de Reglas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
5	Seguridad y Riesgo de la información	o Procedimiento de cambios en la configuración de los dispositivos de seguridad perimetral	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

6	Infraestructura/ Responsable de Aplicaciones	o Documentación de aplicaciones principales y puertos que proveen el servicios	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
7	Seguridad y Riesgo de la información	o Procedimiento de depuración de reglas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
8	Seguridad y Riesgo de la información	o Descripción de responsables de la administración lógica de los equipos de seguridad perimetral	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
9	Seguridad y Riesgo de la información	o Procedimiento de Administración de usuarios y permisos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
10	Seguridad y Riesgo de la información	o Procedimiento de configuración y almacenamiento de logs y alertas y centralización en un correlacionador de eventos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
Red Segura		**Equipos Networking: Switch y router**	
1	Administrador Networking	o Procedimiento de cambios en la configuración del dispositivo	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Administrador Networking	o Procedimiento de ABM de Rutas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Administrador Networking	o Descripción de responsables de la administración lógica	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Administrador Networking	o Procedimiento de Revisión de Rutas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

5	Administrador Networking	o Procedimiento de Administración de usuarios y permisos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
6	Administrador Networking	o Procedimiento de configuración de logs y alertas y centralización en un correlacionador de eventos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
7	Seguridad y Riesgo de la información	· Norma de Seguridad en Comunicaciones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
Red Segura		**Access Point**	
1	Seguridad y Riesgo de la información	o Procedimiento de Configuración de Access Point, cambios en configuración y administración de los dispositivos (siempre y cuando la información de las tarjetas viaje por la infraestructura Wireless)	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
Medidas de Control de acceso		**Configuración de Estaciones de Trabajo**	

Continua

1	Soporte a usuarios	o Procedimiento de configuración de Firewall Personal	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Infraestructura/ Responsable de Aplicaciones	o Procedimiento de configuración de NTP	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Seguridad y Riesgo de la información	o Procedimiento de Instalación/Configuración del Antivirus o formas de despliegue de políticas centralizadas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Seguridad y Riesgo de la información	o Procedimiento de Instalación de actualizaciones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
5	Soporte a usuarios	o Procedimiento de configuración de logs y alertas y centralización en un correlacionador de eventos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
Medidas de Control de acceso		**Configuración de Servidores**	
1	Infraestructura/ Responsable de Aplicaciones	o Procedimiento de configuración del Firewall	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Infraestructura/ Responsable de Aplicaciones	o Procedimiento de configuración de NTP	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Infraestructura/ Responsable de Aplicaciones	o Procedimiento de Instalación/Configuración del Antivirus o formas de despliegue de políticas centralizadas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Infraestructura	o Procedimiento de Instalación de actualizaciones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

5	Infraestructura	o Procedimiento de configuración de logs y alertas y centralización en un correlacionador de eventos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
Seguridad de la Información		**Documentación General**	
1	Administrador Networking	· Disponer de diagrama de la red actualizado, que evidencie los autorizadores de las tarjetas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Seguridad y Riesgo de la información	· Normativa para acceso remoto	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Seguridad y Riesgo de la información	· Normativa para Administración de Usuarios	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

Mantener un Programa de Gestión de Vulnerabilidades		Ambientes de Software	
1	Gerente IT	· Norma de Desarrollo de Software	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Seguridad y Riesgo de la información	o Norma de Separación de Ambientes y Cambios a Software	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Seguridad y Riesgo de la información	o Procedimiento para paso software o desarrollo a producción	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Seguridad y Riesgo de la información	o Proceso y procedimiento para ejecución de cambios o modificaciones de configuración en software	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

Implementar Medidas sólidas de control de acceso		Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información	
1	Seguridad y Riesgo de la información / Recursos Humanos	o Norma / Políticas de control de accesos y seguridad Física	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Seguridad y Riesgo de la información / Recursos Humanos	o Controles de seguridad para acceder a las áreas físicas en las que se encuentra la infraestructura que tiene acceso a los datos de los tarjetahabientes	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Recursos Humanos / Responsable Área Administrativa	o Registro y almacenamiento de Cintas de Seguridad física	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Administrador Datacenter	· Norma para copia de respaldos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

5	Administrador Datacenter	o Proceso de respaldo de información	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
6	Administrador Datacenter	o Inventario de Copia de Respaldos y procedimiento de recuperación	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
7	Seguridad y Riesgo de la información	· Plan de Respuesta ante Incidentes (Debe incluir los procedimientos de Continuidad y Recuperación del Negocio)	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
8	Seguridad y Riesgo de la información	· Política de administración de logs	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
9	Seguridad y Riesgo de la información	· Procedimiento de administración del Antivirus	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
10	Seguridad y Riesgo de la información	· Procedimiento de administración de parches de seguridad	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
11	Seguridad y Riesgo de la información	· Procedimiento para realizar escaneos periódicos de redes inalámbricas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
12	Seguridad y Riesgo de la información	· Procedimiento para realizar escaneos de vulnerabilidades en forma periódica	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
13	Seguridad y Riesgo de la información	· Procedimiento de Configuración del Sistema de Detección de Intrusiones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

14	Seguridad y Riesgo de la información	· Procedimiento de monitoreo del Sistema de Detección de Intrusiones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
15	Recursos Humanos	· Procedimiento de revisión de antecedentes previos a la contratación de nuevo personal	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
16	Seguridad y Riesgo de la información	· Programa formal de concientización de seguridad para los empleados y usuarios internos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
Monitorizar y probar regularmente las redes			
1	Seguridad y Riesgo de la información	· Configuración del Firewall y respaldo de reglas, NATs y rutas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

2	Administrador Networking	· Evidencia de Revisión Semestral de Reglas en los firewall y routers	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
3	Administrador Networking	· Respaldo de configuraciones de los dispositivos	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Administrador Networking	· Registros de Cambios Implementados en los dispositivos de comunicaciones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
5	Administrador Networking	· Plan de Respuesta ante Incidentes	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
6	Administrador Networking	· Procedimientos de Continuidad y Recuperación del Negocio	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
7	Infraestructura	· Registros de Cambios Implementados en la configuración de Servidores, estaciones de trabajo	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
8	Administrador Networking	· Evidencias de pruebas de funcionamiento de contingencia	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
Mantener una Política de Seguridad de la Información			
1	Seguridad y Riesgo de la información	· Política de contraseñas definida: longitud, complejidad, historial de contraseñas, tiempo de expiración	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
2	Gerente IT	· Manejo de correlacionador de Logs de auditoria de todos los componentes del sistema	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

Continua

3	Seguridad y Riesgo de la información	· Escaneos periódicos de redes inalámbricas	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
4	Seguridad y Riesgo de la información	· Escaneos de vulnerabilidades en forma periódica	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
5	Seguridad y Riesgo de la información	· Pruebas de penetración y escaneos recientes	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
6	Seguridad y Riesgo de la información	· Monitoreo del Sistema de Detección de Intrusiones	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
7	Seguridad y Riesgo de la información	· Aceptación de la Política de Seguridad de la Información por parte de los empleados y proveedores	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %

Continua

		Qué se requiere para cumplir el requerimiento?:	
8	Seguridad y Riesgo de la información	· Plan del Programa formal de concientización de seguridad	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	
9	Seguridad y Riesgo de la información	· Pruebas del Plan de Respuesta ante Incidentes	☐ 0 a 25 % ☐ 26 a 50 % ☐ 51 a 75 % ☐ 76 a 100 %
		Qué se requiere para cumplir el requerimiento?:	

3.3.4.2 Resultados de Encuesta

A pesar de la confidencialidad de la información, por tratarse de una encuesta que tiene el único propósito de conocer la realidad de la información que dispone cada área de IT que conforman la entidad bancaria, fue factible obtener resultados de 3 entidades.

Las encuesta fue realizada a personal técnico de las entidades con el carácter de confidencial y no divulgación de información que identifique a la entidad bancaria.

La referencia para valorar el nivel de cumplimiento de las entidades muestreadas es:

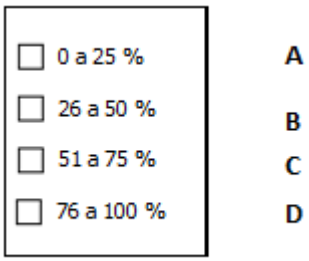


Figura 27 Referencias de porcentajes de cumplimiento

De esta manera los resultados se los muestra en la figura 28:

CATEGORIAS	REQUISITOS	ENTIDAD 1	ENTIDAD 2	E
Desarrollar y mantener una red segura	Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas	A	A	D
	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores	A	B	C
Proteger los datos del titular de la tarjeta	Proteja los datos del titular de la tarjeta que fueron almacenados	B	B	B
	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas	A	A	C
Mantener un programa de administración de vulnerabilidad	Utilice y actualice regularmente el software o los programas antivirus	C	B	D
	Desarrolle y mantenga sistemas y aplicaciones seguras	B	B	B
Implementar medidas sólidas de control de acceso	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio	B	B	B
	Asignar una ID exclusiva a cada persona que tenga acceso por computadora	C	C	C
	Restringir el acceso físico a los datos del titular de la tarjeta	C	A	C
Supervisar y evaluar las redes con regularidad	Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas	A	A	C
	Pruebe con regularidad los sistemas y procesos de seguridad	A	A*	B
Mantener una política de seguridad de información	Mantenga una política que aborde la seguridad de la información para todo el personal	C	B	C

Home: Banco [redacted]

Figura 28 Resultados de Encuesta

** No es factible evidenciar dicho valor de ejecución del requisito.*

Se puede evidenciar el bajo porcentaje de cumplimiento de los requisitos de PCI DSS, de manera que existe una ardua labor para el ente regulador a fin de conseguir un porcentaje elevado de cumplimiento en las entidades bancaria de Ecuador.

Uno de los mayores inconvenientes que se encontró en los resultados de las encuestas es que no existe evidencia de ejecución sin embargo la falencia se da en que no existen procesos o procedimientos formalmente establecidos, la falta de documentación y registro de las actividades ejecutadas provocan el no cumplimiento de determinado requisito.

Gráficamente los resultados son representados en la figura 29:

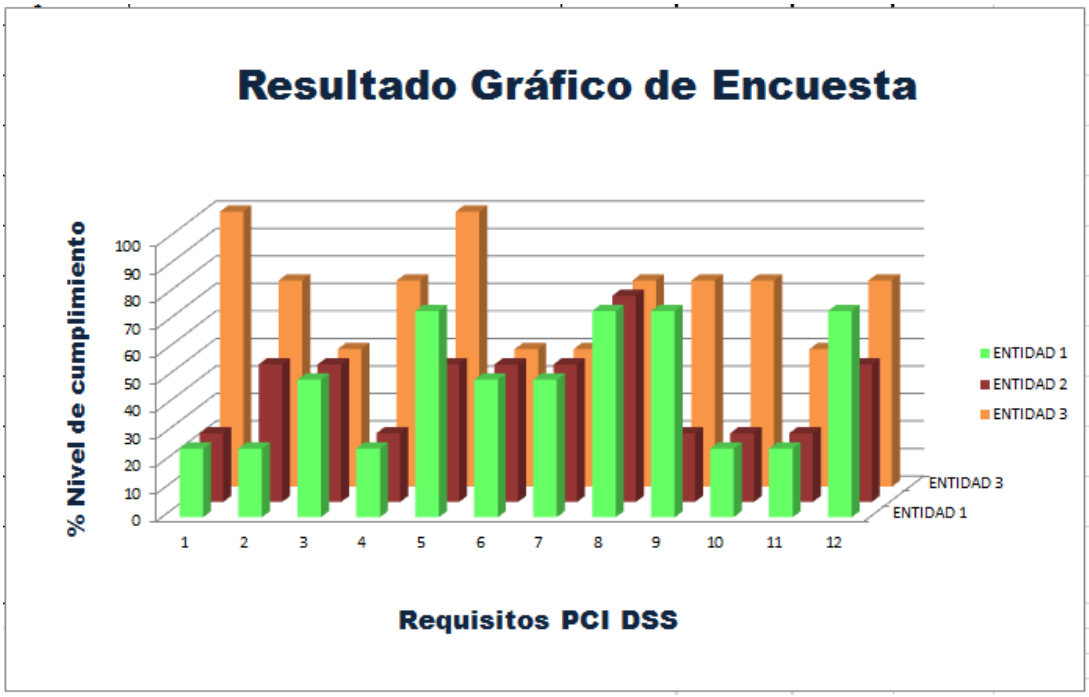


Figura 29 Resultados gráficos de encuesta

Se puede evidenciar el bajo nivel de cumplimiento en solo 3 entidades parte de las muestras, es decir existe un arduo trabajo que realizar para cumplir con los requisitos establecidos por PCI DSS previas a la certificación y considerando que dichos requisitos se deben cumplir al 100 % sin excepción alguna.

CAPITULO IV

Modelo para el análisis de factibilidad de certificación PCI DSS de las entidades bancarias de Ecuador

"Los estándares son siempre obsoletos. Eso es lo que los hace estándares"

---- Alan Bennett

CAPÍTULO IV

MODELO DE ANÁLISIS DE FACTIBILIDAD DE CERTIFICACIÓN PCI DSS DE LAS ENTIDADES BANCARIAS DE ECUADOR

Es importante conocer todos los elementos que participan en el ámbito de la ardua tarea de certificación PCI DSS, se ha mencionado a las tarjetas como el elemento principal a proteger por la información sensible que contiene y que es expuesta en todas las actividades de comercio de los tarjetahabientes. Y por ello se describe sus componentes.

4.1 Elementos y datos sensibles en las tarjetas

Las PCI DSS se aplican donde sea que se almacenen, procesen o transmitan datos de cuentas. Los datos de cuentas constan de los datos de los titulares de tarjetas más datos confidenciales de autenticación, como se detalla a continuación:

Los datos de titulares de tarjetas incluyen:	*Los datos confidenciales de autenticación incluyen:*
• Número de cuenta principal (PAN) • Nombre del titular de la tarjeta • Fecha de vencimiento • Código de servicio	• Todos los datos de la banda magnética o datos equivalentes que están en un chip • CAV2/CVC2/CVV2/CID • PIN/Bloqueos de PIN

Figura 30 Datos de tarjetas

Fuente: (Council P. S., 2012)

El número de cuenta principal es el factor que define la aplicabilidad de los requisitos de las PCI DSS. 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 procesa ni transmite, no se aplican los requisitos de las PCI DSS.

Si el nombre del titular de la tarjeta, el código de servicio y/o la fecha de vencimiento no se almacenan ni procesan ni transmiten con el PAN, ni están presentes de alguna otra manera en el entorno de datos del titular de la tarjeta, se deben proteger de acuerdo con todos los requisitos de las PCI DSS, a excepción de los Requisitos 3.3 y 3.4, que sólo se aplican al PAN.

Las 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 de datos (por ejemplo, el nombre del titular de la tarjeta), o definir las prácticas de divulgación de una entidad en lo que respecta a la información de los consumidores. Entre los ejemplos está la legislación relacionada con la protección de los datos de los consumidores, la privacidad, el robo de identidad o la seguridad de los datos. Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones del gobierno ni otros requisitos legales.

La figura 31, ilustra los elementos de los datos de titulares de tarjetas y los datos confidenciales de autenticación que habitualmente se utilizan; independientemente de que esté permitido o prohibido el almacenamiento de dichos datos y de que esos datos deban estar protegidos. Esta tabla no pretende ser exhaustiva, pero se proporciona con el fin de ilustrar distintos tipos de requisitos que se le aplican a cada elemento de datos.

Los Requisitos 3.3 y 3.4 de las PCI DSS sólo se aplican al PAN. Si el PAN se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN debe ser ilegible de acuerdo con el Requisito 3.4 de las PCI DSS.

		Elemento de datos	Almacenamiento permitido	Hace que los datos de la cuenta almacenados no se puedan leer según el Requisito 3.4
Datos de la cuenta	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación	Datos completos de la banda magnética	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN	No	No se pueden almacenar según el Requisito 3.2

Figura 31 Datos de las tarjetas y su confidencialidad

Fuente: (Council P. S., 2012)

4.2 Ubicación de datos sensibles de las tarjetas

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 PIN5. Estos datos son muy valiosos para las personas malintencionadas, ya que les permiten generar tarjetas de pago falsas y crear transacciones fraudulentas. En la figura 32 muestra las fotografías del reverso y el frente de una tarjeta de crédito, se puede observar la ubicación de los datos del titular de la tarjeta y los datos confidenciales de autenticación.

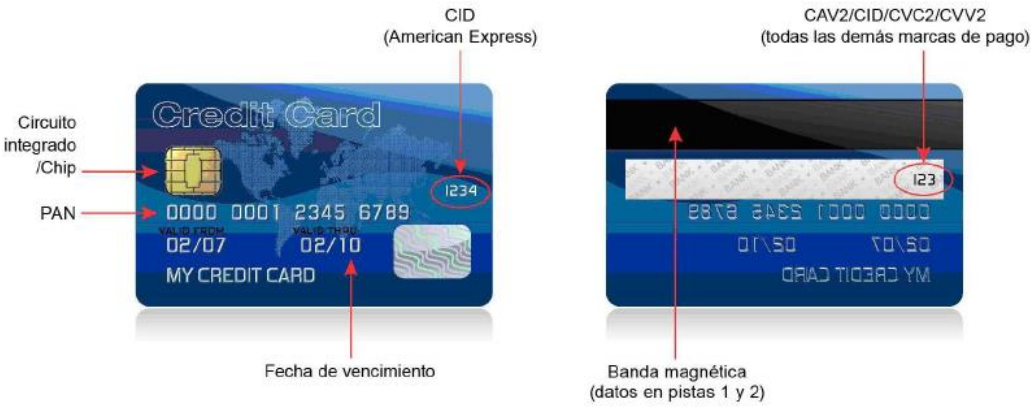


Figura 32 Ubicación de información sensible en las tarjetas

Fuente: (Council P. S., 2012)

El chip contiene datos de pista equivalentes, así como también otros datos confidenciales, incluido el valor de verificación de la tarjeta en el chip de Circuitos Integrados (IC), que también se conoce como Chip CVC[8], iCVV[9], CAV3[10] o iCSC[11]).

El emisor de la tarjeta y/o la marca de la tarjeta de pago definen los campos de Datos discrecionales. Los campos definidos por el agente emisor que contienen datos que el agente emisor/marca de pago considere datos confidenciales de autenticación pudieran estar incluidos en la porción de datos discrecionales de la pista, y pudiera ser posible almacenar estos datos particulares bajo circunstancias y condiciones específicas, tal como lo defina el agente emisor/marca de la tarjeta de pago. Sin embargo, ningún dato considerado dato confidencial de autenticación se puede almacenar después de la autorización, independientemente de si se encuentran en un campo de datos discrecionales o cualquier otro lugar.

Luego de revisar el contexto de elementos y definiciones de PCI DSS para las tarjetas y conociendo que la información no debe ser almacenada, las siguientes son las razones por la cual se almacenan los datos de los tarjetahabientes a pesar de su prohibición:

- Análisis contra fraudes
- Identificación y seguimiento a clientes
- Perfilar clientes, pronósticos de compras
- Business Intelligence
- *Chargebacks*[12] (contracargo)
- Para compartirlos con socios de negocio

[8] Card Verification Value (valor de verificación de la tarjeta) (en Visa y Discover)
9 CVV – Card Verification Value (valor de verificación de la tarjeta) (en Visa y Discover)
10 Card Authentication Value (valor de autenticación de la tarjeta) (en tarjetas de pago JCB)
11 Card Security Code (código de seguridad de la tarjeta) (en American Express)
12 Chargeback es la devolución de fondos a un consumidor, es la reversión de una transferencia previa salida de fondos de la cuenta bancaria de un consumidor, línea de crédito o tarjeta de crédito.

- No hay razón, solo los mantienen en caso de necesitarse en el futuro.

Esta información tan valiosa es buscada por los “Carders” o conocidos como Cyberdelincuentes y su ámbito son los comercios tradicionales, comercios on-line, empresas portadoras de servicios de aplicaciones y sistemas de pago y su intención es obtener:

- Software que almacena datos sensibles de tarjetahabientes
- Información Personal
- Propiedad Intelectual Corporativa
- Track Data (datos de pista) y Números de Cuenta Primarios (PAN)
- Mercado negro de información.
- Distribución global de información de manera instantánea

4.3 Etapas de Aflicción en la implementación de PCI DSS

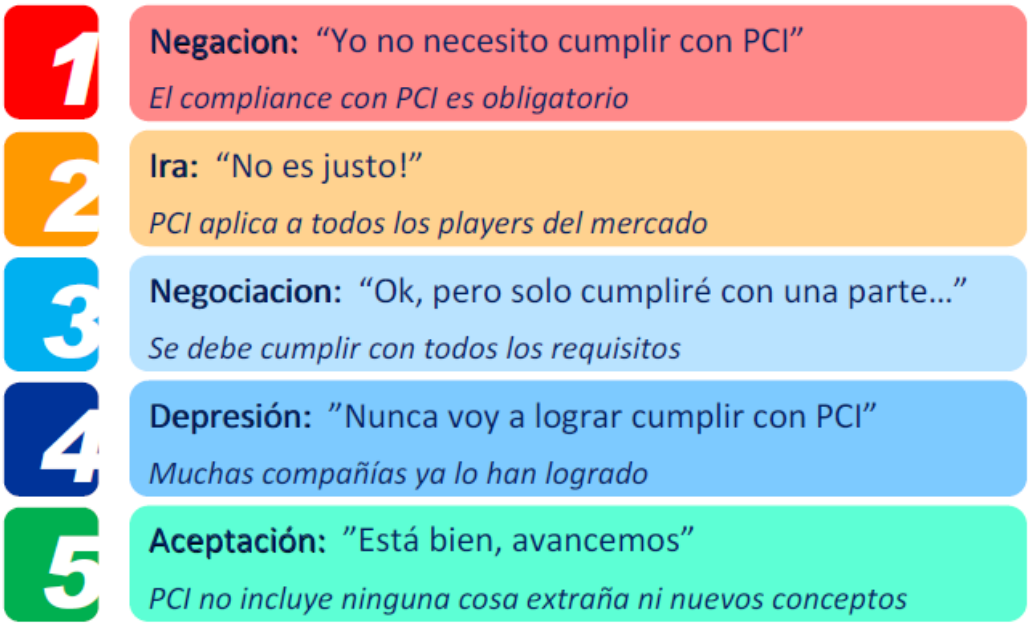


Figura 33 Las 5 etapas del Aflicción de PCI DSS

Fuente: (CYBSEC, 2007)

Hasta el momento se ha realizado el enfoque del marco teórico que es de utilidad para la definición del modelo de análisis de factibilidad en la certificación PCI DSS de las entidades bancarias de Ecuador. Considerando que se trata de un proceso largo y agobiante, PCI SSC hace mención de sus 5 etapas del "de aflicción". La figura 33 resume el significado de cada etapa:

Las entidades bancarias enfocan sus servicios en función de la visión de su negoción que no es la parte de tecnología y es la razón por la cual se tiene cierto temor a la implementación.

La Etapa de la "negación", se presenta dado que hasta el momento las entidades bancarias no tienen la obligación de cumplimiento al no verse afectadas directamente con eventos que atentan con la seguridad de la información de los tarjetahabientes y porque hasta el momento continúan brindando el servicio sin la necesidad de disponer de la certificación.

La etapa de la "ira" se presenta dado la probable errónea información los comerciantes ofrecen servicios y luego se viene la obligatoriedad de cumplimiento de certificación y deben realizar inversiones en algo que no estaba previsto.

La etapa de la "negociación", el intentar una negociación implica el cumplimiento parcial de los requisitos de PCI DSS sin ser esto factible pues para la certificación se deben cumplir estrictamente todos los requisitos.

La etapa de la "depresión", se presenta dado que en ciertas entidades bancarias va a requerir cambios de fondo en la infraestructura de comunicación y ello involucra afectaciones e indisponibilidad de servicios.

La etapa de la "aceptación", se presenta una vez ya iniciado el proceso cuando se tiene claridad de las actividades que se deben realizar y los beneficios que ello aportaran a la entidad bancaria que enfoca sus esfuerzos

en mantener a los clientes satisfechos por los servicios prestados y que los mismos sean seguros.

4.4 Dificultades para Iniciar el Proceso de Certificación

Las dificultades importantes que se encontraran en el proceso son las siguientes:

- Documentación inexistente, incompleta o desactualizada y falta de seguimiento de la misma.
- Desconocimiento del alcance del estándar y las actividades a realizar. Se piensa que PCI es un proyecto de IT y es un proyecto del negocio.
- Manejo del PAN y otros datos de tarjeta. Almacenamiento y procesamiento del mismo.
- Falta de monitoreo sobre los equipos involucrados
- No hay concientización del personal relacionado con el ambiente de tarjetas
- Dificultad de extensión de cumplimiento de PCI a proveedores
- Complejidad de cumplimiento de cuestiones técnicas en entornos propietarios
- Falta de personal para tareas operativas de seguridad, generalmente existe una sola persona encargada de este tema y de infraestructura de red.

4.5 Dificultades en el Proceso de Certificación PCI DSS

Si una entidad bancaria almacena, procesa o transmite información de titulares de tarjetas de pago, sus requisitos de negocio deben cumplir con el Estándar de PCI DSS, en este esquema existen tres cuestiones que en este proceso se torne una situación complicada:

- La primera es que el cumplimiento de los requisitos del Estándar PCI DSS puede afectar a la organización. Es importante coordinar las labores de cumplimiento en todos los departamentos e implantar una estrategia de cumplimiento del Estándar PCI DSS para toda la organización.
- La segunda dificultad es que es posible que la organización deba cumplir con distintos conjuntos de normas, cada uno de los cuales exige el cumplimiento de una serie de requisitos. De hecho, a muchas compañías les cuesta asimilar la forma de responder adecuadamente a esta diversidad de requisitos normativos, al tiempo que usan procesos y procedimientos económicos para el cumplimiento ininterrumpido de las normas.

- La tercera cuestión complicada es que el Estándar PCI DSS, como otras muchas normas, menciona los controles de TI superficialmente, hecho que provoca que los administradores de TI deban determinar exactamente cómo tienen que proceder para cumplir de forma continuada con las normas, con escasa orientación y sin la intervención de un ASV[13].

4.6 Entorno de Análisis para las Entidades Bancarias

La seguridad de la información de tarjetas es una verdadera preocupación en todo el mundo tanto para los bancos que emiten de tarjetas de pago como para los comercios que las aceptan y, por supuesto, para los clientes que las utilizan. La certificación PCI DSS debe convertirse en una prioridad dado que una entidad bancaria es responsable no solo de la seguridad de sus propios sistemas, sino también de la seguridad de los sistemas de su completa red de comercios y de las de sus agentes o servidores de pago según el análisis

[13] ASV, Approved Scanning Vendor

realizado por VISA (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006):

En este entorno es necesario realizar el análisis a una entidad bancaria en los siguientes contextos:

- Dentro de sus propios sistemas
- Dentro de los sistemas de sus comercios
- Dentro de los sistemas de servidores de pago

Permitiendo una compresión del proceso y una visión de planificación de la infraestructura requerida.

4.7 Entorno y términos del ámbito de las tarjetas

Es importante conocer los términos de los participantes del proceso en el cual se manejan las tarjetas y aclarar su relación. La figura 34 muestra cómo se relacionan:

Emisor, es la 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”. (PCI SSC, 2010)

Adquirente, también se lo conoce como “banco adquirente” o “institución financiera adquirente”. Se refiere a la entidad que inicia y mantiene relaciones con los comerciantes para la aceptación de las tarjetas de pago. (PCI SSC, 2010)

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. Tenga en cuenta que un comerciante que acepta tarjetas de pago por bienes y servicios puede ser también un proveedor de servicios, si los servicios comerciados

tienen como resultado almacenamiento, procesamiento o transmisión de datos de titulares de tarjetas a nombre de otros comerciantes o proveedores de servicios. (PCI SSC, 2010)

Figura 34 Participantes del entorno de las tarjetas

Fuente: (PCI SSC, 2010)

Titular de tarjeta, conocido también como tarjetahabiente es el consumidor o no consumidor para el que se emite la tarjeta de pago, o cualquier individuo autorizado para utilizar una tarjeta de pago. (PCI SSC, 2010)

4.8 Modelo propuesto para el análisis de factibilidad de Certificación PCI DSS de Entidades Bancarias

El modelo propuesto tiene la finalidad de encaminar a las entidades bancarias de Ecuador en el proceso de certificación PCI DSS de una manera más ágil y rápida; para que cuando inicien el proceso formal a través de una empresa certificada los costos sean menores, dado que se pretende que los requisitos a cumplir o definir sean menores acortando los tiempos de soporte especializado requerido para el efecto. Se debe considerar que las marcas de tarjetas proponen su propio modelo encaminados en los mismos entornos que

son los intervinientes en el proceso de las tarjetas de pago utilizados como apoyo para el cumplimiento de PCI DSS. El modelo de referencia utilizado es el propuesto por VISA. (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006)

4.8.1.A Quien va Dirigido el Modelo Propuesto

El objetivo de este modelo es ayudar principalmente a los administradores de TI a conocer la forma de encaminar los requisitos de cumplimiento del estándar PCI DSS, el conocimiento del mismo es a nivel general dado que el proceso involucra a todos los miembros de una entidad y por ende se puede destinar a aquellas personas que sean responsables de asegurarse de que sus organizaciones recopilen, procesen, transmitan y almacenen datos de los titulares de tarjetas de forma segura y confiable, al tiempo que mantienen la privacidad de esos titulares; así entre ellos podemos mencionar (o el equivalente de determinada entidad de acuerdo a su organigrama organizacional):

- Directores/Gerentes de información (CIO) encargados de la implementación y el funcionamiento de sistemas y de los procesos asociados a TI.
- Directores/Gerentes de seguridad de la información (CISO) encargados del programa de seguridad de la información global y de las directivas de cumplimiento de la seguridad de la información.
- Directores/Gerentes financieros (CFO) encargados del entorno de control global de sus organizaciones.
- Directores/Gerentes de privacidad (CPO) responsables de la implementación de directivas relacionadas con la administración de la información personal, incluidas las directivas que son compatibles con el cumplimiento de la legislación en materia de privacidad y protección de datos.

- Responsables de la toma de decisiones técnicas que determinan las soluciones de tecnología adecuadas para determinados problemas de la empresa.
- Directores/Gerentes de operaciones de TI que dirigen los sistemas y procesos que ejecutan el programa de cumplimiento del Estándar PCI DSS.
- Arquitectos de seguridad de TI que diseñan los sistemas de control y seguridad de TI para proporcionar un nivel de seguridad adecuado con objeto de cubrir las necesidades empresariales de sus organizaciones.
- Arquitectos de infraestructuras de TI que diseñan infraestructuras que son compatibles con los controles y la seguridad de TI que diseñan los arquitectos de seguridad de TI.
- Consultores y asociados que recomiendan o implementan procedimientos recomendados de privacidad y seguridad para cumplir los objetivos de cumplimiento del Estándar PCI DSS.
- Directores/Gerentes de auditoría de TI encargados de la auditoría de sistemas de TI y de la reducción de la carga de trabajo de los auditores de TI internos y externos.

Considerar que se parte del hecho que en esta etapa ya se conoce a detalle los requisitos a cumplir, mismos que fueron especificados en el Capítulo 2; los requisitos son continuamente analizados por PCI SSC y los cambios son publicados en su sitio oficial: http://es.pcisecuritystandards.org

4.8.2.Detalles previos

La primera pregunta complicada y que más confunde a toda organización es conocer “el nivel actual de la entidad bancaria”. En qué nivel estoy?, resulta la pregunta más importante ya que esto determina el trabajo que se debe realizar para el cumplimiento de la norma PCI DSS, esto es fácil de identificar conociendo los datos de transacciones de la entidad, si se han presentado

eventos que hayan comprometido la información y si alguna marca de tarjeta lo ha identificado como un comerciante nivel 1.

El modo concreto en que las PCI DSS afectan a su negocio y el modo en que deben implantarse dependerán de:

- El tamaño y la naturaleza del propio negocio
- El ámbito y la naturaleza de la red de sus comercios
- El número y el tipo de servidores de pago contratados por el banco y/o por sus comercios.

Para el proceso de implementación encaminada a la certificación, el modelo pretende:

- Guiar, a detalle por todo el proceso
- Ofrecer acceso sencillo e inmediato a toda la información asociada
- Proporcionar detalles de aquellos servidores de pago que ya cumplen las normas y aquellos que se hallan en proceso.
- Proporcionar detalles de los (ASV) Asesores de Seguridad Acreditados

American Express, Discover, JCB, MasterCard o Visa, están sujetos a PCI. El nivel de su organización PCI depende de cuántas transacciones al año procesan la organización. Aunque no es una marca de pago, los proveedores de servicios están directamente involucrados en el procesamiento, el almacenamiento o la transmisión de datos de la tarjeta de pago en nombre de sus clientes u otras organizaciones. Esto incluye a las empresas que prestan servicios (tales como alojamiento web, servicios gestionados, etc) que controlan o podrían afectar a la seguridad de los datos de los tarjetahabientes.

4.8.3.Esquema de Implementación

En la figura 35, se muestra el proceso de implementación encaminada a la certificación de una entidad bancaria, los entornos de análisis deben ser evaluadas en función de cada entidad bancaria y sus propios esquemas de operación dado que son específicos y diferentes uno de otro, probablemente se reduzcan al análisis únicamente de la infraestructura propia de la entidad

bancaria de la cual es directamente responsable y como se mencionó en 4.6, el entorno de análisis es:

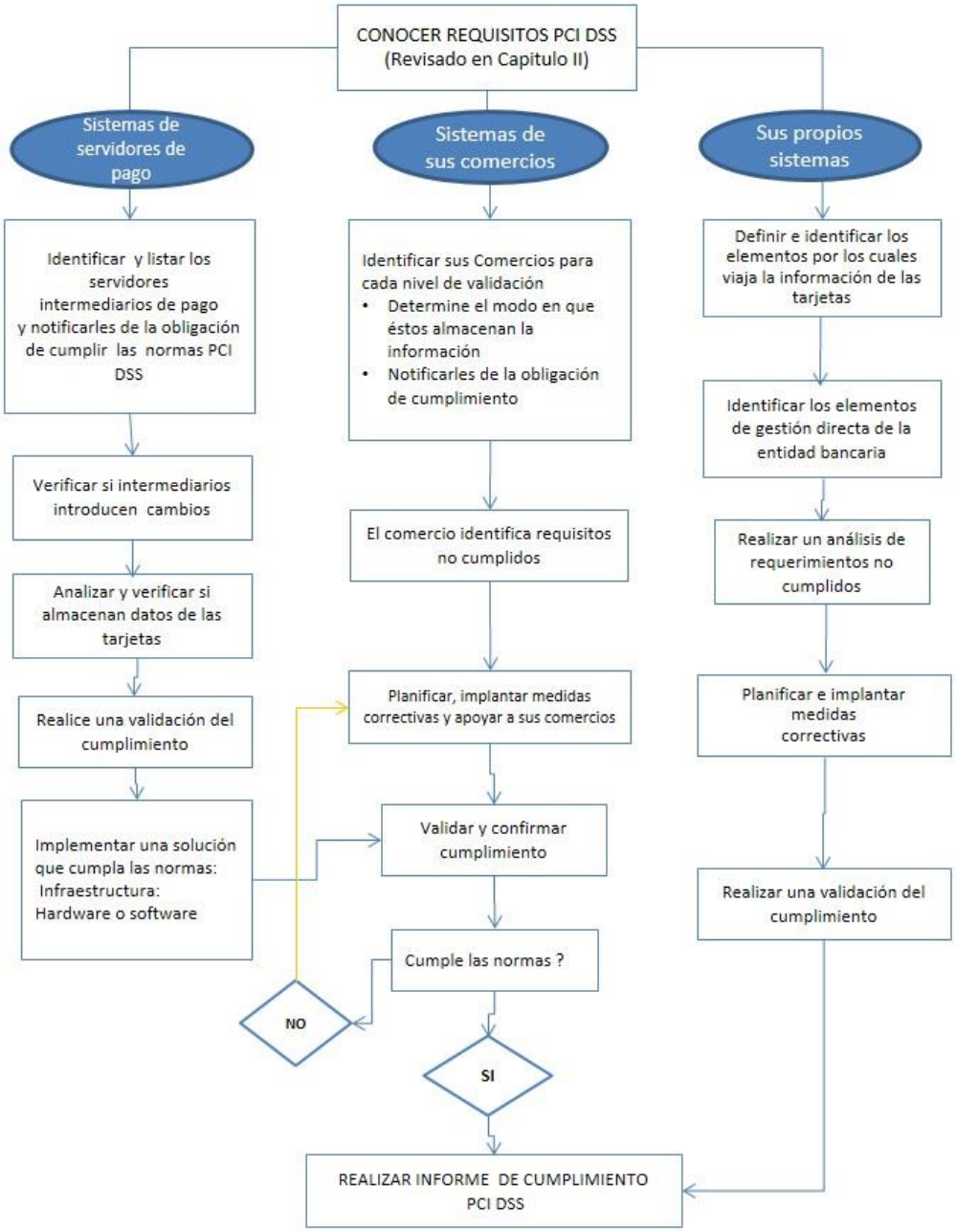


Figura 35 Esquema de análisis para la implementación

4.8.4.Dentro de sus Propios Sistemas:

Los pasos a seguir se los presenta en la figura 36 y a continuación el detalle de cada acción a ejecutar:

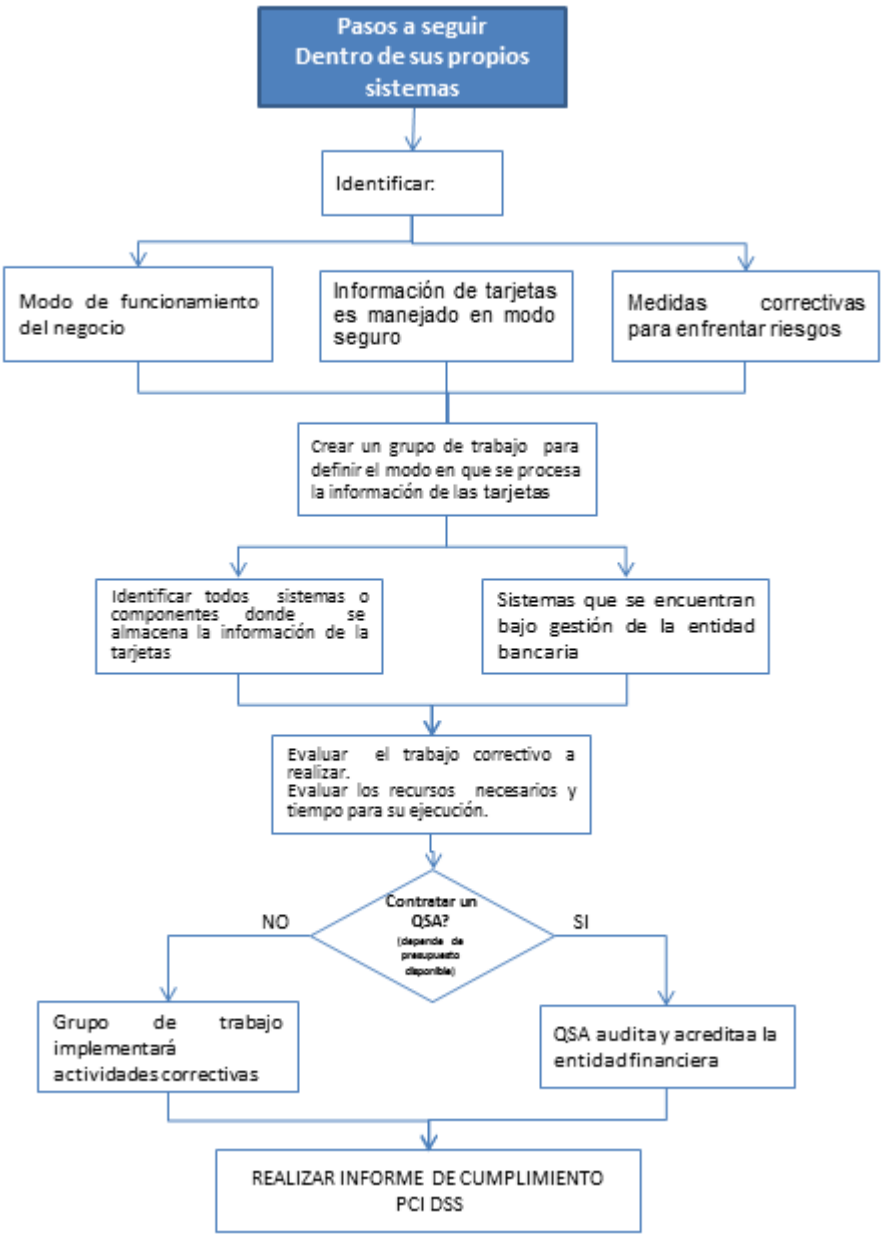


Figura 36 . Pasos a seguir dentro de sus propios sistemas

Fuente: (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006)

Este escenario es el de mayor interés dado que es en el cual la entidad bancaria se verá afectada directamente por los cambios que debe realizar a nivel de su infraestructura y corresponde a los pasos propuestos por VISA. (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006).

4.8.4.1Paso 1. Establecer cómo afecta PCI DSS a sus propios sistemas.

La implementación de las PCI DSS en su propio negocio implica:

- Descubrir de qué modo funciona la información de las tarjetas dentro de su infraestructura.
- Determinar si maneja la información de tarjetas de un modo seguro.
- Poner en práctica medidas correctivas para mitigar los riesgos asociados

Esto ayudará identificar las modificaciones que se requieren a nivel de la infraestructura de comunicaciones que constituye la base para establecer la conectividad y habilitar los servicios. Esta actividad conlleva una serie de actividades que requerirán inversión inicial de recurso humano de distintas áreas a fin de encaminar adecuadamente las actividades a seguir.

4.8.4.2Paso 2. Definir el tráfico de datos de su negocio

Se analizar el modo exacto en que se procesa la información de las tarjetas en los sistemas de la entidad bancaria y definir todos los recorridos de información relacionados.

Los resultados críticos de este de este análisis son:

- Identificará todos los sistemas en los que la información de tarjetas está almacenada
- Revelará cuáles de estos sistemas se encuentran bajo el control directo de la entidad bancaria.

- Evaluar la cantidad de recursos que pueden ser necesarios y el tiempo que llevara para concluir el proceso.
-

Es probable que algunos de estos sistemas se hallen bajo el control de servidores intermediarios de pago o un vendedor. Considerar que la entidad bancaria es responsable, con independencia del lugar y del medio en que se almacene y transmita la información.

En esta fase del proceso, también debe tener en cuenta si debe contratar, y en qué condiciones, los servicios de un QSA[14], para soporte con el cumplimiento de las PCI DSS.

4.8.4.3Cuarto paso: Medidas correctivas y acreditación

Con o sin el soporte de un QSA la entidad bancaria implantará las actividades correctivas necesarias, introduciendo todos los cambios legales, de procedimientos y de sistemas necesarios, a fin de cumplir con PCI DSS.

Considerar que se pretende adecuar y organizar la infraestructura de red encaminada en cumplir los requisitos para la certificación.

Si decide contratar los servicios de un QSA, es recomendable que éste audite y acredite independientemente a la entidad bancaria. Así se verificará si todos sus sistemas cumplen con las PCI DSS. Considerar que el propio equipo de trabajo asignado para el proyecto puede ser el que realice una completa comprobación y un ejercicio de auto-acreditación. El personal que intervenga en esta actividad debe ser seleccionado acertadamente y se sugiere que sean aquellas personas que dispongan de mayor experiencia en la entidad bancaria dado que son los que mayormente aportaran con su conocimiento.

[14] *Qualified Security Assessors*

4.8.5.Dentro de los sistemas de los proveedores de servicios

La figura 37, indica que se debe aliarse con aquellos proveedores contratados directamente por la entidad bancaria y/o con aquellos que trabajan en nombre de sus comercios,

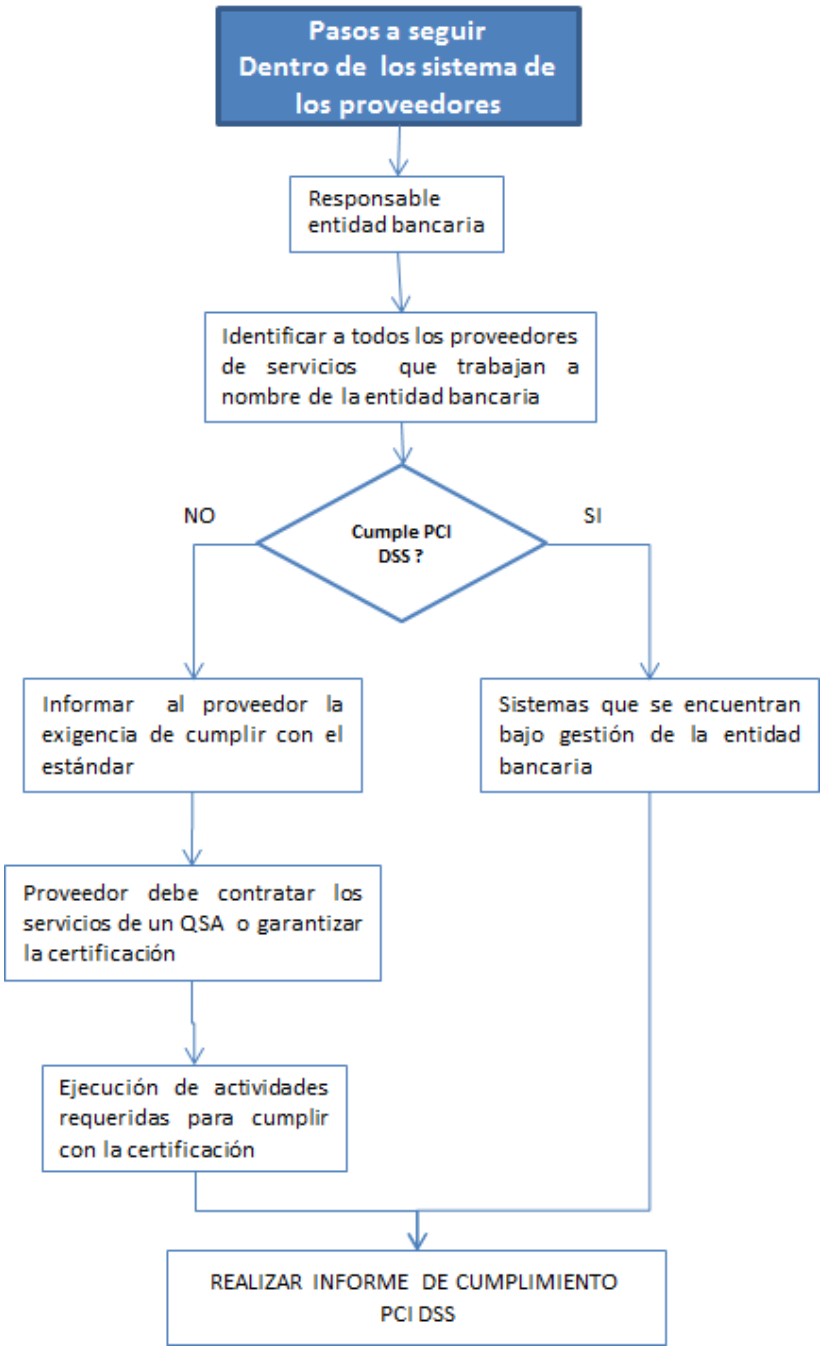


Figura 37 Pasos a seguir dentro de los sistemas de los proveedores

La entidad bancaria es responsable de las actividades de dichos servidores de pago y por tanto, es de su competencia verificar que todos estos servidores de pago cumplen las PCI DSS.

Los pasos a seguir son los recomendados por VISA, (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006) y se los enumera a continuación:

- Identificar a todos los proveedores de servicios de pago y establecer su estatus de cumplimiento
- Identificar y tratar a proveedores de servicios de pago que no cumplen las normas.
- Informar de los proveedores de servicios de pago que no cumplen las normas
- Plan de corrección
- Acreditación

No se los analiza a detalle dado que el proveedor de servicios tendrá que contratar los servicios de un QSA para ayudarle con el cumplimiento de las PCI DSS. Para obtener un listado de QSA´s se recomienda acceder a https://www.pcisecuritystandards.org./approved_companies_providers/qsa_companies.php.

Una vez introducidos los cambios acordados, el proveedor de servicios estará preparado para someterse a una auditoría formal y a un proceso de acreditación, actividades realizadas por el QSA.

Si el proveedor de servicios es un vendedor de programas informáticos, sus productos serán auditados de conformidad a PCI PA-DSS[15]. En otros casos, el proveedor de servicios será auditado de conformidad con las PCI DSS.

[15] Payment Application Data Security Standard

4.8.6.Dentro de los Sistemas de sus Comercios

Dada la preocupación que suscitan los asuntos relacionados con la seguridad de la información de tarjetas, es totalmente necesario que todos los comercios (con independencia del ámbito o la naturaleza de su negocio) cumplan las normas PCI DSS.

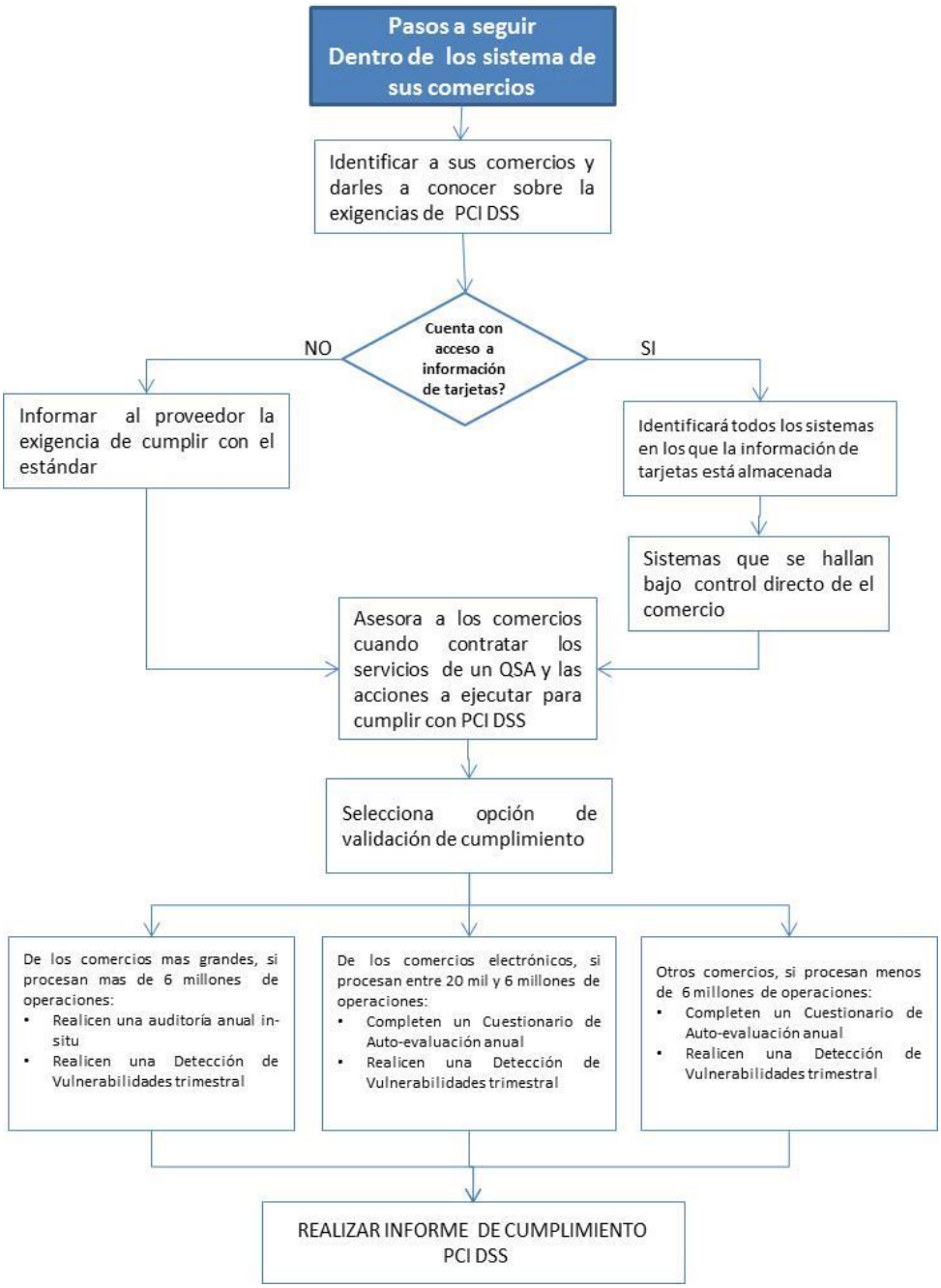


Figura 38 Pasos a seguir dentro de los sistemas de sus comercios

Fuente: (VISA, Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa, 2006)

Es probable que los comercios más grandes o más sofisticados ya conozcan las PCI DSS y sus implicaciones para la entidad bancaria con la que tengan relación. No obstante, necesitarán su ayuda para poner en marcha un plan de acción para el cumplimiento.

También es probable que otros comercios necesiten ayuda y apoyo adicional. Puede que sea necesario proporcionarles información sobre las PCI DSS y sobre cómo afectan a la entidad bancaria y sea necesario guiarles en el proceso.

4.8.6.1 Primer paso: Familiarizar a sus comercios con el estándar a PCI DSS.

El primer paso es asegurarse de que todos los comercios relacionados con la entidad bancaria conocen las PCI DSS y el modo en que éstas afectan.

Como parte de este proceso, será necesario garantizar que todos los gestores de cuentas y representantes de atención al cliente conocen el programa. O encaminarlos a la contratación de un QSA.

4.8.6.2 Segundo paso: Establecer el modo en que procesan los datos los distintos comercios.

Una vez que sus comercios se hayan familiarizado con las PCI DSS, se debe trabajar directamente con cada comercio para averiguar si tiene acceso a la información de las cuentas y si esta información se procesa de un modo seguro. Es decir cada comercio debe ser capaz de proporcionar todos los detalles sobre el modo en que la información de cuentas se transmite entre los distintos sistemas de su propia organización, cuáles de estos sistemas almacenan información y qué terceros (de existir) gestionan información en nombre de la entidad bancaria.

A fin de realizar este ejercicio de un modo eficaz, un comercio tendrá que conocer todos los aspectos de la entidad bancaria (incluidos asuntos relacionados con comercio electrónico, sistema de pedidos por correo/teléfono y canales de ventas personales).

Como la entidad bancaria es último responsable en caso de que surja algún problema, se debe asegurar de que todos los recorridos de información se definen con sumo cuidado y que no se pasa por alto ningún eslabón de la cadena.

En este paso de encontrará dos hechos críticos:

- Identificará todos los sistemas en los que la información de tarjetas está almacenada
- Revelará cuáles de estos sistemas se hallan bajo el control directo del comercio

Dependiendo del ámbito y la naturaleza del negocio de cada comercio, es probable que algunos (o quizá todos) de estos sistemas estén bajo el control de un vendedor o proveedor de pagos (como un vendedor directo, un vendedor de punto de venta (POS), un proveedor de soluciones integradas, un proveedor de servicios de pago por Internet, un intermediario de pagos o una empresa de alojamiento web).

Basándose en este análisis, será necesario apoyar al comercio en dos líneas de acción:

- Todas las acciones que sean necesarias para garantizar que todos los servidores de pago cumplen las PCI DSS (véase la sección 4.8.5 para más detalles)
- Todas las acciones que sean necesarias para implantar las PCI DSS en el propio negocio del comercio (siguientes pasos)

4.8.6.3 Tercer paso: Realizar un análisis de lagunas informativas y establecer el ámbito del proyecto.

Una vez definidos los recorridos de información en la entidad bancaria, el comercio debe identificar cualquiera de sus propios sistemas en los que se almacene información de tarjetas.

Estos sistemas se convertirán en su principal centro de atención. Durante estas etapas iniciales del proceso de implantación, se debe trabajar con el comercio para:

- Obtener orientación sobre el ámbito del trabajo correctivo que puede ser necesario para cumplir las PCI DSS
- Evaluar la cantidad de recursos que pueden ser necesarios y el tiempo que tardará en concluirse el proceso, aproximadamente
- Crear un equipo de proyecto para debatir las respectivas funciones y responsabilidades (como la comunicación con el banco adquirente, la comunicación con los servidores de pago, la especificación de los cambios técnicos, el establecimiento de necesidades de formación, etc.).

En esta fase del proceso, también debe asesorar a los comercios sobre cuándo y en qué condiciones contratar los servicios de un QSA. Es posible que algunos comercios prefieran contratar a un QSA desde el principio del proceso. Puede que otros prefieran realizar el trabajo inicial a nivel interno y recurrir a un QSA en una fase posterior del proceso para que realice una revisión más pormenorizada.

4.8.6.4 Cuarto paso: Seleccionar la opción de validación.

Dependiendo del ámbito del negocio de cada comercio y de la configuración de sus sistemas de aceptación de tarjetas, existen tres formas distintas de comprobar y validar su cumplimiento de las PCI DSS:

- De los comercios más grandes (es decir, los que procesan por lo general más de seis millones de operaciones con tarjeta Visa y/o MasterCard al año) se espera que:

- Realicen una auditoría anual in-situ
- Realicen una Detección de Vulnerabilidades trimestral

- De los comercios electrónicos más grandes (es decir, los que procesan por lo general entre 20.000 y de seis millones de operaciones con tarjeta Visa y/o MasterCard al año) se espera que:
  - Completen un Cuestionario de Auto-evaluación anual
  - Realicen una Detección de Vulnerabilidades trimestral

- De otros comercios (es decir, los que procesan por lo general menos de seis millones de operaciones con tarjeta Visa y/o MasterCard al año) se recomienda que:
  - Completen un Cuestionario de Auto-evaluación
  - Realicen una Detección de Vulnerabilidades trimestral

Basándose en su propia experiencia dentro de su mercado, puede hallarse en una posición espléndida para recomendar cuál de estas opciones es más apropiada para un comercio concreto.

4.8.6.4.1Sobre la auditoria anual in situ.

La auditoría anual in situ es una evaluación de riesgos independiente, generalmente realizada por un QSA. Durante el proceso de auditoría, el Asesor seguirá un procedimiento de comprobación estándar, desarrollado en torno a los 12 requisitos PCI DSS.

Si el comercio recurre actualmente a un QSA para realizar las revisiones in-situ en su nombre, es posible que este mismo asesor pueda realizar también la auditoría in-situ de las PCI DSS. Asimismo, es posible que sea el propio personal del comercio el que realice la auditoría. Dada la experiencia de la entidad bancaria con sus comercios concretos, ocupa una posición extraordinaria para asesorarles sobre la línea de acción más adecuada.

4.8.6.4.2Sobre la Detección de Vulnerabilidades trimestral.

Una Detección de Vulnerabilidades garantiza que los sistemas del comercio están protegidos contra amenazas externas (como el pirateo informático y los virus maliciosos). Las herramientas de detección comprueban todo el equipamiento de la red, los alojamientos y las aplicaciones para detector vulnerabilidades conocidas.

Las detecciones no son intrusivas y las realiza un proveedor de detecciones de seguridad de la red acreditado ASV[16]. El listado de ASV´s se lo puede encontrar en el siguiente sitio:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php?mode=list&page=4

Es necesario realizar detecciones regulares a fin de garantizar que los sistemas y las aplicaciones del comercio continúan aportando los niveles adecuados de protección. Si las detecciones identifican vulnerabilidades, será necesaria una detección de seguimiento para garantizar la eficacia de la medida correctiva adoptada.

4.8.6.4.3Sobre el Cuestionario de Auto-evaluación anual.

El Cuestionario de auto-evaluación es una herramienta gratuita y confidencial que puede utilizarse para medir el nivel de cumplimiento de las PCI DSS por parte del comercio.

El Cuestionario de auto-evaluación es una herramienta online que consta de una serie de preguntas cuya respuesta es “sí” o “no”. Una vez completado el cuestionario, un comercio podrá realizar una buena evaluación de su exposición al riesgo.

Es probable que la mayoría de los comercios deseen descargar la versión imprimible del Cuestionario de autoevaluación y se lo puede encontrar en

[16] Approved Scanning Vendor

http://es.pcisecuritystandards.org/minisite/en/saq-v2.0-documentation.php; antes de enviar sus respuestas.

Así, podrá distribuir las preguntas entre las personas adecuadas de su organización para obtener las respuestas más precisas. A fin de cumplir las PCI DSS, los comercios tendrán que ofrecer respuestas afirmativas a cada una de las preguntas o indicar (cuando esta opción sea válida) que dichas respuestas no se aplican a su negocio.

Es posible que los comercios deseen completar el proceso de auditoría o del Cuestionario de auto-evaluación a nivel interno, o pueden recurrir a un QSA para completarlo en su nombre (o asesorarles en algunos aspectos del mismo).

4.8.6.5 Quinto paso: Planificar e implantar medidas correctivas.

El comercio puede realizar este análisis a nivel interno o recurrir en este punto a los servicios de un QSA. Recurrir a los servicios de un Asesor en etapas tempranas puede añadir un valor significativo al proyecto. El asesor puede ofrecerle una perspectiva experta sobre la sostenibilidad de las actividades correctivas del comercio y la cronología planificada.

En esta etapa, el comercio puede encargar actividades correctivas concretas al personal de la entidad bancaria o a proveedores externos.

Deberá recomendar siempre que el comercio inicie cualquier trabajo correctivo en sus propios sistemas lo antes posible. Desde una perspectiva de gestión de proyectos, puede que sea apropiado esperar hasta que los servidores de pago cumplan las normas. No obstante, no debe olvidarse que el objetivo principal no es acreditar el cumplimiento, sino conseguirlo y mantenerlo.

4.8.6.6 Sexto paso: Acreditación.

A fin de superar la fase de acreditación final, será necesario que los comercios:

- Corrija todos los sistemas que estén bajo su control

- Confirme que todos sus servidores de pago han logrado el pleno cumplimiento (y que han implantado productos y servicios que cumplen las normas dentro de los sistemas de aceptación de tarjetas del comercio)

Una vez hecho esto, llega el momento de que el comercio, bien independientemente o con el soporte de un QSA, realice la auditoría in-situ (o complete el Cuestionario de Auto-evaluación).

El comercio deberá informar a la entidad bancaria, confirmando que ha logrado el cumplimiento.

4.8.7.Método para Identificar Proceso de Cumplimiento en los Comercios.

Para un mejor análisis de los Comercios se propone la aplicación del método de Deming enfocado en el cumplimiento del estándar PCI DSS y se muestra en la figura 39 (Vieites Á, 2007):

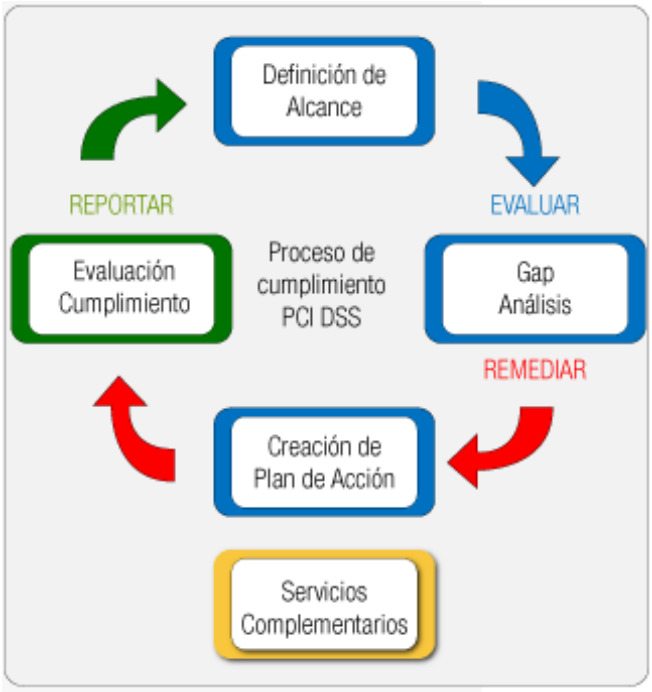


Figura 39 Proceso de cumplimiento PCI DSS

Fuente: (Acosta R., 2012)

Este es el esquema fundamental en cual las empresas dedicadas al soporte (QSAC[17]) en temas de cumplimientos con PCI DSS se orientan, se debe encaminar en un esquema de mejora continua de la seguridad global de los elementos involucrados. Este esquema del proceso a seguir debe ser encaminado en delimitar el entorno afectado, identificar los puntos de no cumplimiento o no conformidad con la norma y ejecutar las acciones que deban tomarse para subsanarlos.

4.8.7.1.Definición del alcance:

Las acciones a realizar en este paso son:

- Identifica los procesos de negocio
- Identificar los canales involucrados en la información de los tarjetahabientes
- Identificar la infraestructura tecnológica que soporta o por la cual atraviesa la información de los tarjetahabientes
- Analizar el alcance de la normativa PCI de manera general para tener una visión contextual y completa de la situación.
- El cumplimiento de los requerimientos aplica a todos los componentes del sistema.
- Un componente del sistema es cualquier elemento de red, servidor, aplicación que esté incluida o conectada al ambiente de datos de los tarjetahabientes.
- El ambiente de datos de los tarjetahabientes (CDE[18]) es la parte de la red que almacena, procesa y/o transmite datos de los tarjetahabientes o información de autenticación.
- Reducir al mínimo donde se almacenan los datos
    - Segmentar la red
    - Restringir el acceso

[17] Qualified Security Assesor Company: empresa autorizada por las PCI SSC para realizar evaluaciones in situ del cumplimiento de las normas PCI DSS.
[18] Card Holder Data Envoriment

4.8.7.2.GAP Análisis:

Las acciones a realizar en este paso son:

- Identificar la brecha existente entre las prácticas tecnológicas de la entidad bancaria y los requerimientos de la norma PCI DSS.
- Identificar si existen restricciones de negocio o técnicas y controles compensatorios para estas restricciones.
- Evaluar todas las áreas relevantes de acuerdo a los requisitos de la normativa en su última versión en este caso versión 2.0 vigente a partir del 2010, con esto conoceremos que falta por cumplir.
- Analizar el manejo del manejo que se da a la información en los procesos relacionados con tarjetas (crédito o débito), en función de la comparación del estado actual y el estado deseado para cumplir con PCI DSS
- Proveer una guía para la toma de decisiones acerca de los procesos y controles técnicos a implementar.
- Provee un método para medir el cumplimiento.
- Definir un plan de acción de los controles a implementar, antes de llevar a cabo la evaluación por parte de una QSA.
- Identificar y documentar el GAF entre donde estás y el Standard Proporciona la base para determinar el tiempo, presupuesto y recursos requeridos

4.8.7.3.Plan de acción:

Las acciones a realizar en este paso son:

- Permite identificar los controles a implementar para obtener el cumplimiento.
- Se prepara un informe donde se muestra el cumplimiento de cada uno de los requerimientos de forma específica, proporcionando una guía clara de los pasos necesarios para alcanzar el cumplimiento de la normativa, en esta fase nos podemos apoyar en la

documentación “Compresión del objetivo de los requisitos” http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/Navigating_DSS_v2.pdf

4.8.7.4.Evaluación de cumplimiento:

Las acciones a realizar en este paso son:

- Evaluar los controles de la norma PCI DSS o los controles compensatorios propuestos con el fin de verificar el cumplimiento y reportar a las marcas.
- Realizar el seguimiento de lo propuesto en el informe GAP de manera de recomendar las soluciones técnicas más viables que se ajusten a las definiciones de los requisitos de PCS DSS.
- Cubre todos los sistemas y comunicaciones que almacenan, procesan o transmiten información de los tarjetahabientes.
- Incluye la identificación de los proveedores de servicio.
- El resultado en un reporte de cumplimiento para ser enviado al Banco o Entidad Adquirente.

4.8.8. Estrategias de Acercamiento a PCI DSS.

A fin de facilitar el cumplimiento de PCI DSS, se debe acudir a estrategias para limitar el ambiente sobre el cual se enfocará los esfuerzos:

4.8.8.1.Remover información sensitiva.

- Remover información sensitiva y bajar los tiempos de retención de información.
- Si no se almacena información sensitiva, el riesgo ante un incidente de seguridad se reduce. El lema es “Si no se necesita, no lo almacene”.

4.8.8.2.Proteger el perímetro.

- Proteger el perímetro, la red interna y las redes wireless.

- Delimitar al máximo posible el “entorno” de red de operación con las tarjetas.
- Se debe segmentar la red interna.
- No debe permitirse el acceso desde Internet hacia la red de operación de tarjetas.
- Se deben utilizar mecanismos de autenticación y encriptación fuertes en redes wireless (WPA2).

4.8.8.3.Asegurar las aplicaciones de medios de pago.

- Se deben asegurar los sistemas operativos y las aplicaciones.
- Se deben evitar el uso de protocolos que envíen la información en plano (ftp, http, etc.).

4.8.8.4. Monitorear y controlar el acceso a los sistemas.

- Activar los logs (registro de eventos) a nivel de networking, sistemas operativos y las aplicaciones para poder detectar “quién, qué, cuándo y cómo” en el uso del ambiente de tarjetas.
- Unificar los logs, zona horaria y horario.
- Centralizar y correlacionar eventos.

4.8.8.5. Proteger la información almacenada de las tarjetas.

- Para las organizaciones que deben almacenar el PAN por su forma de operación, se deben implementar mecanismos de protección definidos.

4.8.8.6.Finalizar el resto de los ítems de control.

- Finalizar la parte documental, incluyendo políticas, normas y procedimientos para la operación.
- Asegurarse que los controles se encuentran operativos.

4.8.9. Detalles del Cuestionario de Autoevaluación SAQ[19] .

A fin de cumplir las PCI DSS, los comercios tendrán que ofrecer respuestas afirmativas a cada una de las preguntas o indicar (cuando esta opción sea válida) que dichas respuestas no se aplican a su negocio. Revisado en 4.8.6.4.3

Es necesario identificar el SAQ que servirá de soporte para identificar el cumplimiento de los requisitos definidos por PCI DSS, de acuerdo a:

- SAQ A: Está orientado a las necesidades de los comerciantes que han externalizado todo el almacenamiento, procesamiento y transmisión de la información del titular de la tarjeta.
- SAQ B: Creado para satisfacer las necesidades de los comerciantes que procesan la información del titular de la tarjeta, únicamente mediante máquinas de impresión o terminales independientes de acceso telefónico.
- SAQ C: Construido para orientarse a las necesidades de los comerciantes cuyos sistemas de aplicaciones de pago están conectados a Internet.
- SAQ D: Diseñado para satisfacer las necesidades de todos los proveedores de servicios definidos por una marca de pago como elegibles para completar un SAQ, y de aquellos comerciantes que no entran dentro de las categorías a las que se destinan los SAQ A, B, o C.

Esto lo podemos evidenciar de modo gráfico en la figura 40:

[19] SAQ Self-Assessment Questionnaire

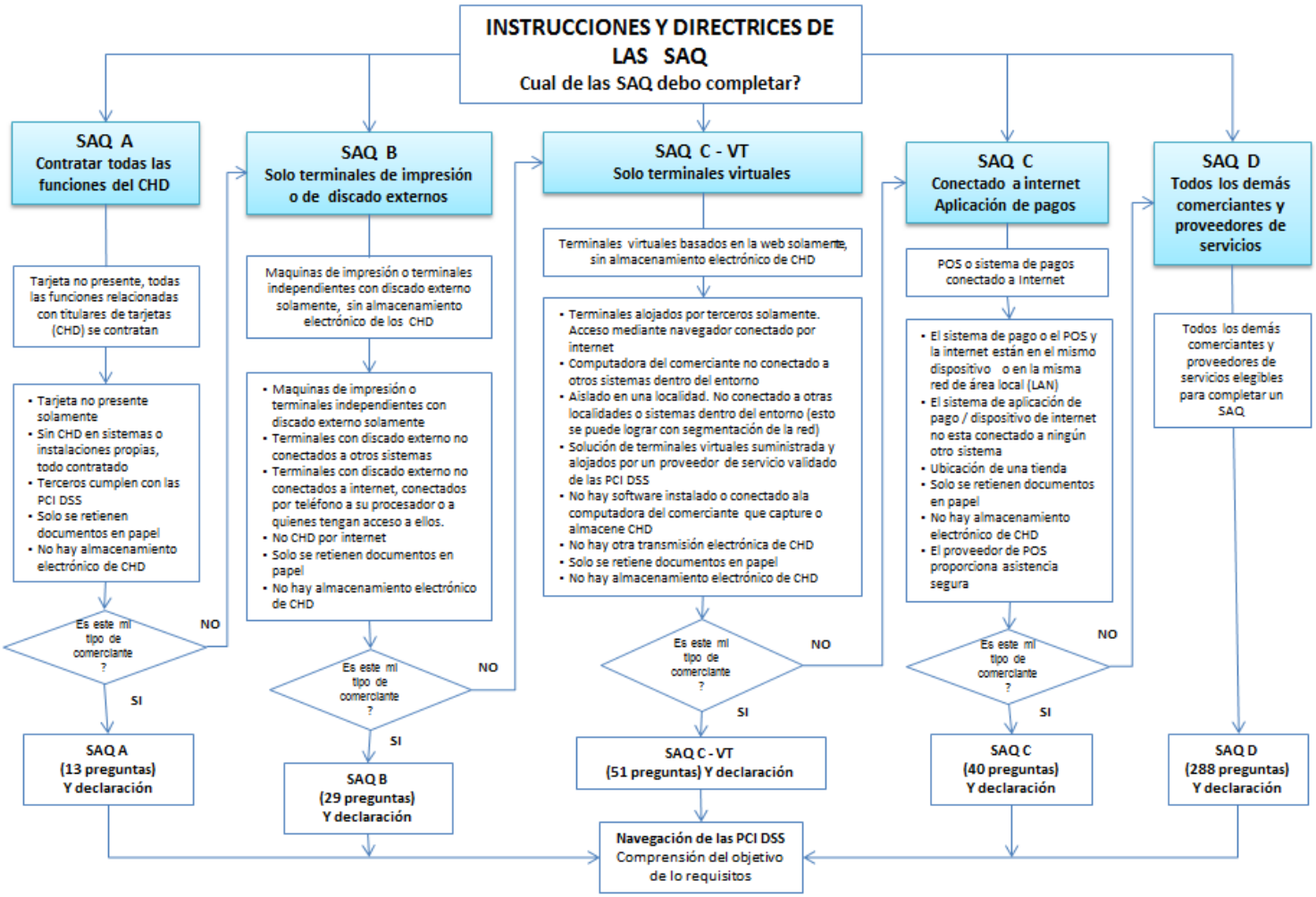


Figura 40 Directrices SAQ

4.9 Proceso de Auditoría del Estándar PCI DSS

El proceso de auditoría para cumplir el Estándar PCI DSS tiene algunos detalles específicos, por tanto es necesario detallarlo a fin de que los encargados del proceso de certificación tengan conocimiento de las etapas de ejecución.

Los análisis de auditoría los realizan dos tipos de organizaciones de terceros, conocidas como asesores de seguridad calificados (QSA)[20] y proveedores de servicios de escaneo aprobados (ASV)[21]. Los evaluadores QSA realizan la parte in situ de la auditoría, mientras que los proveedores ASV realizan los exámenes de vulnerabilidad en los entornos de Internet de la organización. *El organismo PCI Data Security Council (PCI DSC)* se encarga de la evaluación anual de las empresas que se convierten en QSA o ASV para su certificación correspondiente.

El evaluador QSA es necesario para preparar un informe posterior a la auditoría de la organización; este informe debe seguir unas directrices concretas definidas por el PCI DSC. Estas directrices se encuentran en un documento con procedimientos de auditoría de PCI que puede descargar en http://es.pcisecuritystandards.org/minisite/en/pci-dss-v2-0.php).

Las directrices especifican la forma en que se debe organizar el informe que el evaluador QSA debe archivar después de la auditoría. Este informe incluye información de contacto de la organización, la fecha de la auditoría, un resumen ejecutivo, una descripción del ámbito de trabajo y el enfoque que adoptó el evaluador QSA para realizar la auditoría en la organización, resultados trimestrales del examen, y los hallazgos y las observaciones del evaluador QSA. La última sección contiene la mayor parte de la información

[20] *Qualified Security Assessors*
[21] *Approved Scanning Vendors*

acerca del cumplimiento del Estándar PCI DSS de la organización. En ella, el evaluador QSA usa una plantilla para informar acerca del cumplimiento de cada uno de los requisitos principales y secundarios del Estándar PCI DSS por parte de la organización.

Antes de programar las auditorías del Estándar PCI DSS para la organización, o mejor, a medida que planea el cumplimiento del Estándar PCI DSS, los miembros clave de la organización deben revisar los procedimientos de auditoría específicos. Esta medida le puede ayudar a comprender completamente lo que analiza el evaluador QSA durante la auditoría.

El proveedor ASV también debe preparar un informe acerca de los resultados de los exámenes de vulnerabilidad realizados en los entornos de Internet de la organización. Las directrices para la creación de este informe se encuentran en un documento de procedimientos para el examen PCI, que se puede descargar en:

https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v2.0.pdf (en inglés). Este documento especifica los elementos que el proveedor ASV debe examinar en el entorno de la organización e incluye una clave que ayudará a leer e interpretar el informe del proveedor ASV.

Como comerciante o proveedor de servicios, deberá seguir cada requisito del informe de cumplimiento de las respectivas compañías de tarjetas de pago para asegurarse de que cada una de estas compañías es consciente del estado de cumplimiento de su organización. Con otras palabras, si su organización es un proveedor de servicios que administra datos de titulares de tarjetas Visa y American Express, debe enviar los informes de cumplimiento a Visa y a American Express.

4.10 Infraestructura de red recomendada para PCI DSS

La infraestructura de red es específica y propia de cada entidad bancaria pues la misma depende de la tecnología, del personal, del flujo de datos, requerimientos legales, interconexión de sistemas y redes, servicios ofrecidos, virtualización, etc; por tanto resulta complicado generalizar o definir la topología de red recomendada. Sin embargo se describe una red en la que se aplican los controles definidos por PCI DSS en la cual se considera un flujo de datos de tarjetas seguro permitiendo una visión a partir de la cual se puede iniciar la validación de un QSA (Qualified Security Assessor).

En la topología de la figura 41 podemos distinguir los siguientes segmentos de red considerando que la segmentación es una recomendación:

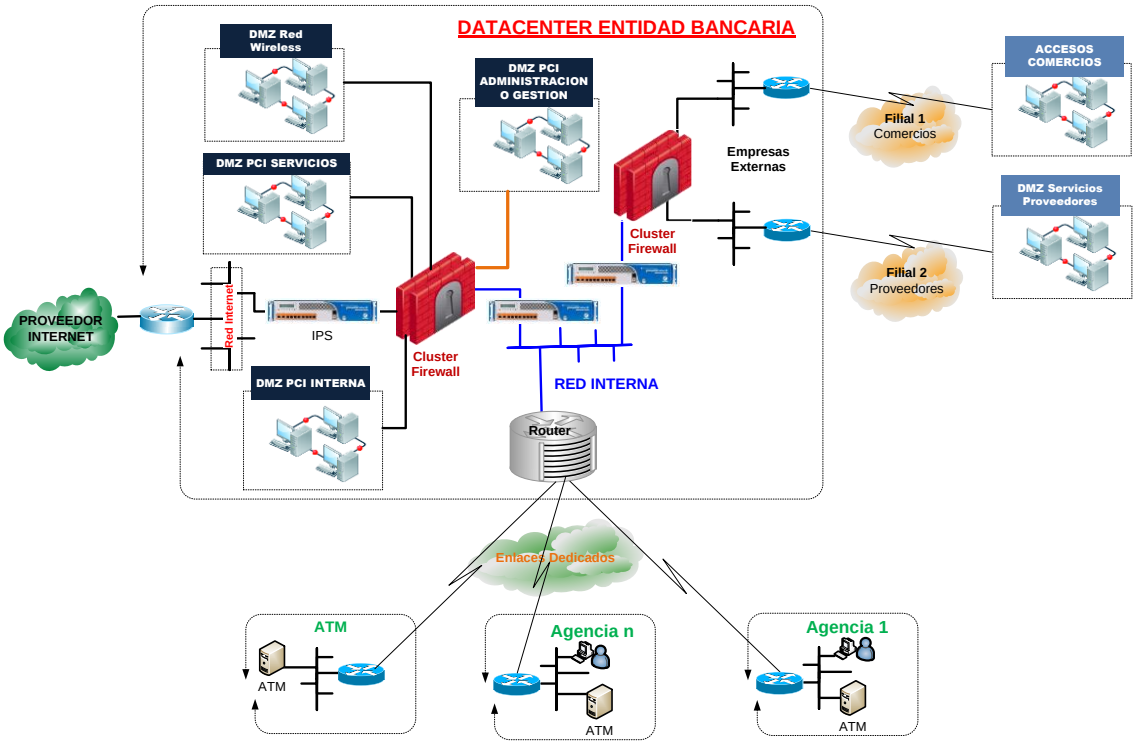


Figura 41 Topología de Red recomendada PCI DSS

DMZ PCI SERVICIOS, considerar una zona en la que se puede instalar equipos que reciben y/o envían datos de tarjetas a redes externas; servidores NTP si se da la necesidad de sincronizar servidores NTP externos y un proxy cuando los servidores de esta DMZ requieren acceso a internet. Como referencia se hace cumplimiento a los REQUISITOS PCI DSS 1.3.1; 10.4.3 y 1.3.8

RED EXTERNA – INTERNET: limita el entorno de la tarjetas de pago y donde se puede colocar los equipos de seguridad perimetral, enrutamiento; también es posible hacer uso de esta zona para conexión por terceros (filiales o empresas externas) sin embargo lo recomendado es hacer uso de otro firewall, se puede colocar equipos concentradores de VPNs, IPs / IDS/ DDOS, filtrado de contenido sea en hardware y/o software en diferentes equipos o en un equipo modular. Como referencia se hace cumplimiento a los REQUISITOS PCI DSS 4.1; 2.2.1

RED GESTION PCI: En este segmento se debe colocar todos las consolas de administración de los servicios de seguridad como antivirus , firewalls, proxys, etc. Así como servers NTP, Syslog, LDAP, RADIUS y cualquier conexión administrativa de la infraestructura de red. Como referencia se hace cumplimiento a los REQUISITOS PCI DSS 8.3; 1.4

DMZ PCI INTERNA: se debe considerar la zona más crítica del ámbito de las tarjetas de pago dado que se puede colocar base de datos, repositorios de claves. Como referencia se hace cumplimiento a los REQUISITOS PCI DSS 1.3.7

DMZ RED WIRELESS: En los componentes inalámbricos que interactúen en el ámbito de las tarjetas de pago se debe implementar los requisitos 1.2.3; 2.1.1 y 4.1.1 que hacen referencia a esta tecnología.

En la actualidad los productos existentes en el mercado que son parte de la infraestructura de red están encaminados y diseñados con la finalidad de cumplir con los requisitos de PCI DSS, los proveedores que tiene relación a brindar servicios de hardware y software se han empeñado en ofrecer productos adaptables a las necesidades de las entidades bancarias y poder cumplir en mayor número con los requisitos de PCI, lo importante es la administración de la infraestructura pues si las políticas y configuraciones no están definidas correctamente indistintamente del equipamiento difícilmente se puede cumplir con los requisitos y serán parte de las observaciones que realizará el QSA.

4.11 Retorno de la Inversión en la Implementación PCI DSS.

Debido al costo que implica la implementación de PCI DSS, cobra especial interés el definir claramente el alcance y la identificación de los elementos afectados, dado que una adecuada segmentación de la red, eliminando datos innecesarios, aislando los sistemas es posible reducir costos y esfuerzo.

El modelo descrito es que se utiliza a nivel de tecnologia considerando que no se espera un retorno monetario; y de acuerdo (Molinero, 2011) se ttiene:

4.11.1Justificación de la inversión.

Ahora la discusión radica en conocer que se gana con la implementación de PCI DSS y cómo justificar la inversión, considerando que cualquier inversión requiere un análisis previo que incluye el cálculo del retorno de dicha inversión (ROI[22]), pero en este caso no podemos medirlo como si se tratara de la creación de nuevas sucursales o nuevos productos o servicios. Si la inversión se refiere a seguridad de la información es habitual calcular el ROSI (*Return On Security Investment*), su cálculo se basa en dos conceptos: costo de la inversión y disminución del riesgo conseguida con dicha inversión. Bajo estas premisas, es factible demostrar que la implementación del estándar PCI DSS

[22] Return of Investment

es económicamente viable ya que la disminución del riesgo conseguida es mayor, en términos económicos, que el costo de la inversión realizada.

4.11.2 ROI vs ROSI

El cálculo del retorno de inversión (ROI) se define como la relación existente entre el costo de una inversión realizada y el beneficio obtenido. Se suele expresar como un porcentaje y se utiliza para calcular la viabilidad de un proyecto. Simplificándolo, un proyecto con ROI positivo será económicamente viable, ya que retornará al inversor más dinero que el que inicialmente invirtió. Por el contrario, un proyecto con ROI negativo será económicamente no viable, ya que no devolverá al inversor ni siquiera la cantidad que invirtió inicialmente lo cual implica que el proyecto debe ser modificado o rechazado dependiendo de su naturaleza o criticidad. La fórmula básica para calcular el retorno de una inversión es (Molinero, 2011):

ROI = (Beneficio - Costo)/Costo

Como se mencionó ámbito de proyectos de seguridad el parámetro "beneficio" debe ser remplazado por "Disminución de Riesgo" a la que esta expuesta la organización que es en realidad el beneficio que la organización alcanzara luego de la implementación. Así, se define el término para el cálculo del retorno de inversión de un proyecto de seguridad de la información ROSI (Return On Security Investment) y la fórmula para su cálculo es la siguiente (Molinero, 2011):

ROSI = (Disminución de Riesgo - Costo)/Costo

La rentabilidad de una inversión en seguridad se espera que sea una disminución del riesgo al que está expuesta la organización. La disminución del riesgo se calcula conforme a la siguiente fórmula (Molinero, 2011):

Disminución del Riesgo = Riesgo Expuesto x %Riesgo Mitigado

El riesgo expuesto se determina por la cantidad de ocurrencias de incidentes de seguridad, así como por el impacto económico causado por cada incidente ocurrido. El riesgo expuesto se calcula, habitualmente, como una tasa anual:

Riesgo Expuesto = Costo de un incidente x Tasa de Ocurrencia Anual

4.11.3 ROSI en la adecuación a PCI DSS.

Se presentan varias interrogantes referentes a que la implementación del estándar PCI DSS, es rentable?, es medible económicamente la disminución del riesgo? ¿Se puede valorar económicamente el retorno de la inversión realizada para adaptar las organizaciones a la normativa PCI DSS?. Estas interrogantes las podemos resolver calculando el ROSI de la implementación del estándar PCI DSS y es necesario obtener el valor de los dos conceptos (Molinero, 2011):

- Costo del proceso de adecuación / implantación, y,
- Disminución del Riesgo, como resultado del alineamiento de la organización con el estándar PCI DSS.

4.11.4 Cálculo de la disminución del riesgo.

El costo de un incidente de seguridad relacionado con tarjetas de pago es un dato que las organizaciones no lo publican y no se dispone de históricos que registren estos eventos. En Ecuador no se dispone de esta información dado que las entidades bancarias no publican esta información y es considerada confidencial precautelando el alto impacto que esto tendría en su imagen (Molinero, 2011).

Como ya se detalló, el cálculo de la disminución del riesgo se lo realiza con las siguientes definiciones:

Disminución del Riesgo = Riesgo Expuesto x %Riesgo Mitigado

Riesgo Expuesto = Costo de un incidente x Tasa de Ocurrencia Anual

De los incidentes ocurridos se puede conocer el riesgo expuesto multiplicándolo por el costo de cada uno de éstos en el año. El riesgo expuesto para entidades que trabajan con tarjetas de pago (crédito o débito) depende de los siguientes parámetros:

- Multa de la entidad emisora de la tarjeta.
- Costo de la investigación forense del incidente.
- Costo de reemplazar las tarjetas.
- Costo del fraude realizado.
- Costo de sanciones relativas a entidades de supervisión local o costos legales
- Costo de la pérdida de productividad de los empleados.
- Costo de la restitución de imagen de marca.

4.11.5 Cálculo del coste de implantar PCI DSS.

La implantación de la normativa PCI DSS en cualquier organización implica tres costos básicos:

- Costo de consultoría (análisis situación inicial o análisis gap, valoración de riesgos, diseño del plan de acción).
- Costo de adaptación de sistemas y procesos a PCI DSS (implantación del plan de acción que define las tareas para solventar los no cumplimientos).
- Costo de la auditoría de cumplimiento (auditoría on site anual que debe ser realizada por un QSA *Qualified Security Assessor*).

4.11.6 Cálculo del retorno de inversión en la implantación de PCI DSS.

El retorno de la inversión está dado por el ROSI:

ROSI = (Disminución de Riesgo - Costo)/Costo

Con este valor podemos determinar el tiempo en el cual se puede considerar que se recuperará la inversión realizada y se debe considerar que el tiempo se incrementará si la fase de implementación demora aunque en ese supuesto habría que tener en cuenta el coste del mantenimiento de la certificación (Molinero, 2011).

4.12 Ejemplo práctico para el cálculo del ROSI aplicado a PCI DSS

A fin de explicar el cálculo del retorno de la inversión para la implementación del estándar PCI DSS en una organización, se presenta un ejemplo práctico con costos y situaciones específicas, considerando que para efectos reales se debe analizar rigurosamente la entidad de forma independiente. Se considera la moneda en Euros en función de la tabla de la marca propuesta en el ejemplo.

- Se trabajará en función de las siguientes premisas:
  - Entidad Nivel 2
  - Posee un volumen transaccional de alrededor 5 millones anuales, es decir aproximadamente 14000 transacciones diarias
  - Se supone que se presentó un solo incidente de seguridad que involucra tarjetas de pago y fue detectado con 7 días de retraso.
  - Solo el 30% de las tarjetas fueron comprometidas.
  - Número de tarjetas 45.800

4.12.1 Calculo del riesgo expuesto.

- Costo de la multa de la entidad emisora de la tarjeta:

Para el cálculo de este factor se hace uso del programa de multas comprometido y establecido por la marca de las tarjetas en este caso específico VISA de acuerdo a la tabla 8:

Tabla 8

Multas VISA en caso de incidente con tarjetas de pago[23]

Entidad Comprometida	Multa Inicial (€)	Remediación insuficiente después de 90 días	Mensual por infringir PCI DSS (después de 4 meses)	Mensual por infringir PCI DSS (después de 5 meses)	Mensual por infringir PCI DSS (meses subsiguientes)
Nivel 1	€ 50.000,00	€ 30.000,00	€ 50.000,00	€ 75.000,00	€ 75.000,00
Nivel 2	€ 25.000,00	€ 15.000,00	€ 25.000,00	€ 50.000,00	€ 50.000,00
Nivel 3	€ 10.000,00	€ 5.000,00	€ 10.000,00	€ 15.000,00	€ 15.000,00
Nivel 4	€ 10.000,00	€ 5.000,00	€ 10.000,00	€ 15.000,00	€ 15.000,00

Fuente: (Molinero, 2011)

Si la entidad en el momento de producirse el incidente no haya iniciado ningún programa de certificación PCI DSS y considerando que su implementación en promedio dura 1 año, la multa impuesta ascendería a:

730.000 = 50.000 + 30.000 + 50.000 + 75.000 + (7x75.000)

Considerar que un año después la entidad debe demostrar su cumplimiento.

- Costo de la investigación forense del incidente:

La entidad que sufre el incidente de seguridad relacionado con tarjetas de pago debe hacerse cargo de los costos de la investigación forense exigida por VISA, se debe presentar un informe preliminar a los tres días y en función de la gravedad la auditoria puede extenderse a varios días o semanas. Se estima un costo promedio de 15000 euros.

- Costo para remplazo de tarjetas:

En casos de incidentes de seguridad, la entidad deberá asumir los costos de remplazo de las tarjetas. Se estima un costo promedio de 2 euros por tarjeta.

91600 EUROS = 45.800 x 2

[23] http://www.isecauditors.com/sites/default/files/files/SIC95_ISecAuditors_ROI_PCI_DSS.pdf

- Costo del fraude realizado.

Este costo puede ser eliminado si la entidad posee un seguro antifraudes; en este caso se asume que si lo poseía y valor es 0.

- Costo de sanciones relativas a entidades de supervisión local o costos legales

En función del valor que las tarjetas puedan representar en cuanto a demandas de pago dictaminadas por la superintendencia de bancos debido a reclamos de los usuarios; se asumirá un valor mínimo de 1 euro por tarjeta:

45800 EUROS

- Costos improductivos:

Este valor se lo atribuye al personal que no podrá realizar sus funciones diarias debido a que debe atender a los auditores y dedicar sus esfuerzos para solventar el incidente, se asume un valor aproximado de 1 euro por tarjeta comprometida.

45800 EUROS

- Costos de restitución de la imagen de marca

Es una inversión dedicada a realizar campañas de marketing con la finalidad de evitar deserción de clientes debido al incidente a fin de mejorar la imagen de la institución financiera. Se asume 50.000 EUROS

El valor total es del incidente en las condiciones indicadas es: 978.200 EUROS

Para conocer el valor de la disminución del riesgo, se toma en cuenta que PCI DSS disminuirá el 80% del riesgo:

ROSI= *(Disminución de Riesgo - Costo)/Costo; para lo cual:*

Riesgo Expuesto =978.200 EUROS

Riesgo Mitigado = 80%

Disminución del Riesgo = 978.200 x 0.8 = 782.560 EUROS

4.12.2 Calculo del costo de implementación de PCI DSS.

Este valor es un propio y especifico de cada entidad analizada y dependen directamente del nivel de seguridad implementado; por tanto si al iniciar cada proyecto se implementa la solución enmarcada en los requisitos de PCI DSS y se disponga de un mayor número de elementos de seguridad menor será el costo de la inversión (Molinero, 2011).

Dada la complejidad y la demanda de personal y tiempo que implica la implementación de PCI DSS, se recomienda contratar un auditor PCI QSA a fin que realice un análisis quien apoyara en conocer las acciones a realizar y a determinar los costos de implementación interna, costo de la certificación y pagos anuales para mantenerla (Molinero, 2011):

- Costo de asesor QSA

Se requiere su contratación para iniciar los trabajos de análisis, se debe considerar que mientras más apegadas estén las soluciones tecnológicas a los requisitos de PCI menor será el tiempo y costo del asesor. Se considera un costo de 15.000 EUROS

- Costo de la implementación

Se trata de las acciones a ejecutar para cumplir con los requisitos de PCI en función del análisis del QSA y depende de las implementaciones tecnológicas de cada entidad. Se asumen 450.000 EUROS.

- Costo de la auditoria final PCI

Se considera el análisis una vez ejecutadas las acciones recomendadas por el QSA, se asume 10.000 EUROS

Así, tenemos un total de 475.000 EUROS y finalmente:

ROSI = (*782.560 – 475.000) / 475.000*

ROSI = 64.75 % (valor considerado como favorable)

Es necesario considerar que involucra costos que probablemente no sean entendidos a nivel administrativo y gerencial, sin embargo el hecho de mejorar la imagen de la entidad involucra oportunidades de negocio y de garantizar la confianza y fidelidad de los clientes dado el hecho de que se garantiza que los procesos internos de la entidad aseguran la información de las tarjetas de pago de sus clientes.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

"Para triunfar en la vida, no es importante llegar primero. Para triunfar simplemente hay que llegar, levantándose cada vez que se cae en el camino"

— Goeth

CAPÍTULO V

CONCLUSIONES

- Cumplir con el estándar PCI DSS no significa sólo acreditarse o cumplir con las auditorías periódicas, sino establecer un estado en nuestro entorno de pago con tarjetas que cumpla con el estándar en todo momento. De esta forma, en caso de producirse un incidente, la entidad bancaria podrá demostrar que estaba operando bajo los requerimientos establecidos por PCI DSS.

- En Ecuador las entidades bancarias han iniciado un proceso de certificación PCI DSS por cuanto implica el cumplimiento de las normas internas establecidas por la Superintendencia de Bancos y Seguros; actualmente solo un Banco dispone de esta certificación, Banco de Guayaquil es el primer banco que obtuvo esta certificación en diciembre del 2011 en un proceso que duró 2 años.

- El modelo de factibilidad propuesto es viable para las entidades bancarias por cuanto es una descripción de los paso a seguir y los ámbitos a considerar en el proceso, si bien es cierto son descripciones generales los mismos están enmarcados en la realidad de la infraestructura común en una entidad bancaria en función de los resultados de las encuestas realizadas, con el propósito de reducir los costos y acortar los plazos en el proceso de certificación.

- Contar con un programa que cumpla con el estándar PCI DSS ayuda a:
    - Protegerse ante responsabilidades y costos potenciales vinculados a posibles casos de fraude con la información de

tarjetas de pago, costos de investigación en caso de incidente, costos legales, etc.

- Gestionar y controlar la inversión en seguridad de la información.
- Aumentar la confianza de los clientes: un cliente que paga con tarjeta sabe que sus datos están gestionados según un estándar de seguridad.
- Crear una cultura de seguridad en la entidad bancaria.

- El cumplimiento de la normativa PCI DSS es responsabilidad ineludible, no opcional, de todos las entidades que manejan información de las tarjetas de pago incluyendo comercios, comercio electrónico, venta por correo, venta por teléfono, procesadores de pagos, bancos y proveedores de servicios (independientemente del tamaño del negocio); independientemente del número de transacciones de tarjetas de pago procesadas. Sin embargo, los requerimientos de información varían en función del nivel de las transacciones que se procesan por año.

- El cumplimiento de PCI DSS puede integrarse con el sistema de gestión de seguridad de la información (SGSI) de las entidades bancarias a través de ISO27001 y pasar a ser un elemento más en el día a día de la gestión de seguridad de la entidad.

- Para efectos de auditoría y evaluación, PCI SSC homologa empresas como *Qualified Security Assessors (QSAs),* personas encargadas de realizar una revisión del sistema y reportar al ente solicitante los resultados del análisis y *Approved Scanning Vendor (ASV)*; empresas dedicadas a realizar escaneos de seguridad externos. Dependiendo del nivel de transacciones con tarjetas de pago que la organización realice anualmente, se deben realizar escaneos de seguridad trimestrales por un ASV, estar sujetos a auditoría anual por parte de un QSA o

diligenciar un *Self-Assessment Questionnaire (SAQ)*, para garantizar que los controles se encuentran satisfactoriamente desplegados y son monitoreados en forma continua.

- La viabilidad económica de realizar una inversión para adaptar la infraestructura tecnológica de una entidad bancaria en base a los requisitos de PCI DSS y que este método revele un retorno de inversión en un tiempo determinado debe ser estudiado detenidamente en cada caso concreto, considerando que la implantación de PCI DSS no conseguirá rédito económico (ganancia monetaria) como en el caso de inversiones tales como la apertura de una nueva agencia pero de seguro lo que se conseguirá es la fidelidad de sus clientes al contar con el respaldo de que su banco dispone de certificaciones de seguridad a nivel internacional.

RECOMENDACIONES

- Se recomienda que las entidades bancarias encaminen el cumplimiento de PCI DSS como una prioridad dentro de sus proyectos anuales, dado que existe un riesgo y exposición constante a la pérdida de información sensible de las tarjetas de pago; dicha pérdida ocasionará sanciones, acciones legales, mala publicidad y pérdidas económicas.

- La Superintendencia de Bancos y Seguros del Ecuador como ente controlador a través de sus normativas debe dar énfasis al cumplimiento de las disposiciones normativas para exigir a las entidades bancarias controladas la implementación de medidas de seguridad sustentados en los requisitos de PCI DSS.

- Los administradores de red o los responsables del diseño de la infraestructura tecnológica de las entidades bancarias deben enfocar sus diseños en base a las recomendaciones del Capítulo 4 y centrarse en entender el flujo de los datos de la tarjeta de pago: donde se obtienen, procesan, almacenan y transmiten. Deben tener los conocimientos del estándar PCI DSS dado que la base de un análisis correcto se realizará una segmentación de red adecuada para limitar la exposición de los datos de tarjetas de pago reduciendo el alcance de la evaluación del estándar PCI DSS y al mismo tiempo ahorrando significativo en tiempo y costos de inversión para el proceso de certificación.

- Se recomienda que se invierta tiempo en conocer los diferentes requisitos y el alcance de los mismos, esta información está disponible en el sitio web oficial de PCI Security Standards, la implementación de un estándar suele ser bastante costosa por tanto se deben encaminar acciones que en lo posible no sean erróneas. Los estándares como PCI-DSS son genéricos por naturaleza: describen qué hacer, pero no cómo hacerlo; es decir, enfocar los requisitos genéricos del estándar hacia productos y acciones concretas se deja como tareas que debe realizar cada entidad bancaria, de acuerdo a las condiciones particulares de su infraestructura tecnológica.

- Se recomienda realizar mayor énfasis en el Requisito 11 considerado como el aspecto PCI-DSS más difícil de implementar para las entidades pues se refiere al análisis de vulnerabilidades, pruebas de infiltración y uso de un sistema de detección de intrusos, pero el principal motivo de esta dificultad es la falta de experiencia que existe en estos campos, así como el costo que típicamente representa para las empresas implementar un sistema de detección profesional.

- Se recomienda considerar las estrategias de acercamiento a PCI DSS descritas en el Capítulo 4 para facilitar la implementación del estándar en las entidades bancarias de Ecuador; así como considerar el esquema de implementación dentro de los 3 sistemas descritos en el modelo de factibilidad para encaminar a la certificación de dichas entidades.

GLOSARIO

Adquirente

También se conoce como “banco adquirente” o “institución financiera adquirente”. Se refiere a la entidad que inicia y mantiene relaciones con los comerciantes para la aceptación de las tarjetas de pago.

AES

Abreviatura de “Advanced Encryption Standard” (norma de cifrado avanzado).

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

Datos de cuentas

Los datos de cuentas constan de los datos de titulares de tarjetas más los datos confidenciales de autenticación. Consulte Datos de titulares de tarjetas y Datos confidenciales de autenticación

DDoS

Un "ataque por denegación de servicio" (DoS, Denial of service) tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo

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.

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.

Emisor

Entidad que emite tarjetas de pago o realiza, facilita o respalda servicios de emisión incluidos, a modo de ejemplo, bancos y procesadores emisores.

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.

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.

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.

PAN

Acrónimo de “primary account number” (número de cuenta principal), también denominado “número de cuenta”. Número exclusivo de una tarjeta de pago (en general, de tarjetas de crédito o débito) que identifica alemisor y la cuenta específica del titular de la tarjeta.

PCI

Acrónimo de “Payment Card Industry” (Industria de tarjetas de pago).

POS

Acrónimo de “point of sale” (punto de venta). Hardware y/o software que se utiliza para procesar transacciones con tarjetas de pago en la ubicación del comerciante.

PTS

Acrónimo de “PIN Transaction Security” (Seguridad de la transacción con PIN), PTS es un conjunto de requisitos de evaluación modular administrados por el PCI Security Standards Council, para terminales POI con aceptación de PIN. Por favor, consulte www.pcisecuritystandards.org.

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.

PCI DSS

Procedimiento

Narración descriptiva de una política. El procedimiento equivale a los pasos de una política y describe cómo debe implementarse una determinada política.

QSA

Acrónimo de “Qualified Security Assessor” (evaluador de seguridad certificado), empresa autorizada por las PCI SSC para realizar evaluaciones in situ del cumplimiento de las normas PCI DSS.

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

Redes inalámbricas (Wireless)

Red que conecta computadoras sin necesidad de una conexión física de cables.

SAQ

Acrónimo de “Self-Assessment Questionnaire” (Cuestionario de autoevaluación). Herramienta utilizada por una entidad para validad su cumplimiento con las PCI DSS.

Seguridad de la información

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

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.

BIBLIOGRAFÍA

ABPE. (2013). *Información entidades financieras privadas de Ecuador.* Obtenido de Boletin Informativo # 34: http://www.asobancos.org.ec/ABPE_INFORMA/No.34.pdf

Acosta R., D. E. (2012). *Gestión de eventos y monitoreo.* Obtenido de http://www.isecauditors.com/sites/default/files/files/ACIS-Sistemas_100_Gestion_de_eventos_y_monitoreo_en_el_estandar_pci_dss.pdf

BANRED. (2011). *El RETORNO DE LA INVERSION DE LA IMPLEMENTACION PCI-DSS.* Obtenido de http://www.banred.fin.ec/cms2a80.html?c=1291

Camara de Comercio, G. (2012). *Estadísticas entidades financierasCámara de Comercio*. Obtenido de http://www.lacamara.org

Council, P. S. (2012). *PCI DSS*. Obtenido de https://www.pcisecuritystandards.org

Council, S. S. (2012). *SECURING THE FUTURE OF PAYMENTS TOGETHER.* Obtenido de https://www.pcisecuritystandards.org/

CSO. (2012). *Revista mensual Chief Security Officer.* Obtenido de http://www.csoonline.com/

CYBSEC. (15 de Marzo de 2007). *PCI: La nueva Estrategia deSeguridad de las Compa Seguridad de las Compañías de Tarjetas de Pago.* Obtenido de http://www.cybsec.com/upload/PCI_segurinfo_2007.pdf

El Telégrafo, D. (2012). *Banco de Guayaquil recibe un certificado sobre seguridad de datos de los clientes*. Obtenido de http://www.telegrafo.com.ec/economia/item/banco-de-guayaquil-recibe-un-certificado-sobre-seguridad-de-datos-de-los-clientes.html

Eterovic, J. E., & Pagliari , G. A. (15 de Enero de 2011). *Metodología de Análisis de Riesgos Informáticos*. Obtenido de http://www.cyta.com.ar/ta1001/v10n1a3.htm

INEC. (2012). *Estadísticas anuales*. Obtenido de http://www.inec.gob.ec/estadisticas/

ITU, U. I. (2012). *Medición de la Sociedad de la Información.* Obtenido de http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2012-SUM-PDF-S.pdf

Marañon, G. Á., & Pérez García, P. P. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: McGraw-Hill.

Molinero, J. M. (Junio de 2011). *Retorno de inversión de PCI DSS.* Obtenido de http://www.isecauditors.com/sites/default/files/files/SIC95_ISecAuditors_ROI_PCI_DSS.pdf

NetMarketing, E. (2010). *Estadísticas nacionales*. Obtenido de http://ecuadorinternetmarketing.wordpress.com/

Normativa ISO 2700. (s.f.). Obtenido de HTTP://www.iso2700.es

Ortiz, L. M., Robalino, C., Benalcazar Alarcon, P., & Vásquez, J. (16 de Enero de 2012). SBS trabaja para crear una cultura de seguridad para banca en línea. (R. Muñoz, Entrevistador)

Palma, L. (2011). *Introducción Seguridad informática.* Mexico: ITESM.

PCI SSC, P. S. (2010). *Glosario de términos, abreviaturas y acrónimos.* Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI%20Glossary.pdf

SBS, S. S. (26 de Abril de 2012). *RESOLUCIÓN JB-2012-2148.* Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

SuperIntendencia de Bancos y Seguros. (2012). *SuperIntendencia de Bancos y Seguros*. Obtenido de http://www.sbs.gob.ec

Superintendencia de Bancos y Seguros, S. (20 de Octubre de 2005). *NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO.* Obtenido de http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

Vieites Á, G. (2007). *Enciclopedia de la Seguridad Informática.* Mexico: Alfaomega Grupo Editor, S.A. de C.V.

VISA. (2006). *Implantación de las Normas de Seguridad de la Información en la Industria de Medios de Pago (PCI DSS) Visa.* Obtenido de http://www.visaeurope.es/visa-para-comercios/seguridad-de-la-informacion-ais

VISA. (2006). *Normativa Operativa de Visa International*. Obtenido de www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity