GUÍA DE IMPLEMENTACIÓN DE HERRAMIENTAS TECNOLÓGICAS DIRIGIDA A LAS PYMES PARA DAR CUMPLIMIENTO A LA NORMA INTERNACIONAL PCI DSS V3.0

ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE FIREWALL DE RED, IPS, NTP, FILTRADO DE CONTENIDO, DLP, DESCUBRIMIENTO DE DATOS DE TARJETA, FIREWALL DE APLICACIÓN, MONITOREO DE INTEGRIDAD DE ARCHIVOS, ESCÁNER DE VULNERABILIDADES, ANTIVIRUS Y CIFRADO DE DATOS, PARA EL CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA DE SEGURIDAD DE DATOS PCI DSS V3.0 QUE EXPLÍCITAMENTE IMPLICAN ADQUIRIR E IMPLEMENTAR HERRAMIENTAS TECNOLÓGICAS DE SEGURIDAD INFORMÁTICA PARA SU CUMPLIMIENTO

HUGO ALEJANDRO CASALLAS LARROTTA
JAVIER PERDOMO VALDERRAMA
JULIO ALBERTO VARGAS FERNÁNDEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2015

GUÍA DE IMPLEMENTACIÓN DE HERRAMIENTAS TECNOLÓGICAS DIRIGIDA A LAS PYMES PARA DAR CUMPLIMIENTO A LA NORMA INTERNACIONAL PCI DSS V3.0

ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE FIREWALL DE RED, IPS, NTP, FILTRADO DE CONTENIDO, DLP, DESCUBRIMIENTO DE DATOS DE TARJETA, FIREWALL DE APLICACIÓN, MONITOREO DE INTEGRIDAD DE ARCHIVOS, ESCÁNER DE VULNERABILIDADES, ANTIVIRUS Y CIFRADO DE DATOS, PARA EL CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA DE SEGURIDAD DE DATOS PCI DSS V3.0 QUE EXPLÍCITAMENTE IMPLICAN ADQUIRIR E IMPLEMENTAR HERRAMIENTAS TECNOLÓGICAS DE SEGURIDAD INFORMÁTICA PARA SU CUMPLIMIENTO.

HUGO ALEJANDRO CASALLAS LARROTTA
JAVIER PERDOMO VALDERRAMA
JULIO ALBERTO VARGAS FERNÁNDEZ

Trabajo de grado para optar al título de
Especialista en Seguridad informática

Asesor
ÁLVARO ESCOBAR ESCOBAR
Ingeniero de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

Firma de Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C. Febrero de 2016

DEDICATORIA

Ante todo, gracias al que todo lo hace posible Dios, jefe de los Ingenieros e inspiración de este proyecto, a nuestras familias por su apoyo y motivación incondicional, y a nuestro asesor ingeniero Álvaro Escobar Escobar por su aporte a nuestra formación profesional y personal.

AGRADECIMIENTOS

Los Autores expresan sus agradecimientos a:

Álvaro Escobar Escobar, director del proyecto

A la Universidad Piloto de Colombia

A todas aquellas personas que de una u otra forma colaboraron en la elaboración de este proyecto

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACCESO REMOTO[1]: acceso a redes informáticas desde una ubicación remota, en general localizada fuera de la red. Las redes VPN constituyen un ejemplo de tecnologías de acceso remoto.

ADMINISTRACIÓN DE CLAVES[2]: en criptografía, se refiere al conjunto de procesos y mecanismos que respaldan el establecimiento y mantenimiento de las claves, así como el reemplazo de claves anteriores por nuevas claves, según sea necesario.

AES[3]: abreviatura de "AdvancedEncryption Standard" (norma de cifrado avanzado). Cifrado por bloques utilizado en la criptografía de clave simétrica que adoptó el NIST en noviembre de 2001 como U.S. FIPS PUB 197 (o "FIPS 197").

ANTIVIRUS[4]: programa o software capaz de detectar y eliminar los diferentes tipos de programas maliciosos (también conocidos como "malware"), incluidos virus, gusanos, troyanos o caballos troyanos, spyware, adware y rootkits, y de proteger su computadora contra estos.

APLICACIÓN[5]: incluye todos los programas o grupos de programas de software adquiridos y personalizados, así como también las aplicaciones internas y externas (por ejemplo, aplicaciones web).

APLICACIÓN WEB[6]: una aplicación a la que generalmente se accede mediante un explorador web o a través de servicios web. Las aplicaciones web pueden estar disponibles a través de Internet o en una red privada e interna.

BASE DE DATOS[7]: formato estructurado que permite organizar y mantener información de fácil recuperación. Algunos ejemplos simples de base de datos son las tablas y las hojas de cálculo.

---

[1]PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 1
[2] Ibid. p. 1
[3] Ibíd. p. 1
[4] Ibíd. p. 2
[5] Ibid. p. 2
[6] Ibíd. p. 3
[7] Ibíd. p. 3

CIFRADO DE DISCO[8]: técnica o tecnología (ya sea de software o hardware) que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). También se utiliza el cifrado a nivel de archivo y el cifrado de bases de datos a nivel de columna para cifrar el contenido de archivos o columnas específicas.

CIFRADO[9]: proceso para convertir información en un formato ilegible, a excepción de los titulares de una clave criptográfica específica. El cifrado se utiliza para proteger la información entre el proceso de cifrado y el proceso de descifrado (lo contrario del cifrado) de la divulgación no autorizada.

CONSOLA[10]: pantalla o teclado que permite obtener acceso al servidor, equipo mainframe u otro tipo de sistema y controlarlo dentro de un entorno de red.

CRIPTOGRAFÍA[11]: disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.

DATOS DE CUENTAS[12]: 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.

DATOS DE LA BANDA MAGNÉTICA[13]: también denominados “datos de pistas”. Datos codificados en la banda magnética o el chip que se utilizan para la autenticación y/o autorización durante las transacciones de pago. Puede ser la imagen de la banda magnética de un chip o los datos de la pista 1 y/o pista 2 de la banda magnética.

DMZ[14]: 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.

[8]PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 4
[9] Ibíd, p. 4
[10] Ibíd, p. 7
[11] Ibíd. p. 9
[12] Ibíd., p. 9
[13] Ibíd., p. 9
[14] Ibíd., p.11

DSS[15]: acrónimo de “Data Security Standard” (norma de seguridad de datos), también denominada “PCI DSS”.

FIREWALL[16]: 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.

IDS[17]**:** acrónimo de “intrusión detection system” (sistema de detección de intrusiones). Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad detectado.

IPS[18]**:** acrónimo de “intrusión prevention system” (sistema de prevención de intrusiones). El IPS va un paso más allá que el IDS y bloquea el intento de intrusión.

IPSEC[19]**:** abreviatura de “Internet Protocol Security” (protocolo de seguridad de Internet). Norma para asegurar las comunicaciones IP mediante el cifrado y/o la autenticación de todos los paquetes IP. IPSEC brinda seguridad en la capa de red.

LAN[20]**:** acrónimo de “local área 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.

NAT[21]**:** acrónimo de “network address translation” (traducción de direcciones de red). Llamada simulación de red o simulación IP. Cambio de la dirección IP utilizada dentro de una red por una dirección IP distinta conocida dentro de otra red.

[15] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 11
[16] Ibíd.,p.12
[17] Ibíd., p.14
[18] Ibíd.p.15
[19] Ibíd.,p.15
[20] Ibíd.,p.15
[21] Ibíd.,p.16

NTP[22]: acrónimo de “network time protocol” (Protocolo de tiempo de red). Protocolo usado para sincronizar los relojes de sistemas informáticos, dispositivos de red y otros componentes del sistema.

NÚMERO DE CUENTA[23]: consulte Número de cuenta principal (PAN).

PAN[24]**:** 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 al emisor y la cuenta específica del titular de la tarjeta.

PCI[25]: acrónimo de “Payment Card Industry” (Industria de tarjetas de pago).

PROTOCOLO[26]: método acordado de comunicación utilizado en las redes. Son las especificaciones que describen las reglas y los procedimientos que deben seguir los diferentes productos informáticos para realizar actividades en una red.

PRUEBA DE PENETRACIÓN[27]: las pruebas de penetración tienen como objetivo explotar vulnerabilidades a fin de determinar la posibilidad de accesos no autorizados u otras actividades malintencionadas. Las pruebas de penetración incluyen pruebas de aplicaciones y redes y controles y procesos de redes y aplicaciones. Se realizan tanto desde el exterior de la red hacia el interior (pruebas externas) como en el sentido contrario.

RED DE CONFIANZA[28]: red de una organización que la empresa es capaz de controlar o administrar.

REDES INALÁMBRICAS[29]: red que conecta computadoras sin necesidad de una conexión física de cables.

RED PRIVADA[30]: red establecida por una organización que utiliza un espacio de dirección IP privado. Generalmente, a las redes privadas se las denomina redes de área local. El acceso a redes privadas desde redes públicas debe estar protegido adecuadamente mediante firewalls y routers.

---

[22] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 17

[23] Ibíd., p.17

[24] Ibíd., p.18

[25] Ibíd., p.18

[26] Ibíd., p.19

[27] Ibíd., p. 19

[28] Ibíd.,p.21

[29] Ibíd.p.21

[30] Ibíd.,p.21

RED PÚBLICA[31]: red específicamente implementada y operada por un proveedor de telecomunicaciones con el propósito de ofrecer al público servicios de transmisión de datos. Los datos que se transfieren por medio de redes públicas pueden ser interceptados, modificados y/o redirigidos mientras están en tránsito. Algunos de los ejemplos de redes públicas para las que rigen las PCI DSS son Internet y las tecnologías móviles e inalámbricas.

REGISTRO DE AUDITORÍA[32]**:** también denominado "pista de auditoría", corresponde al registro cronológico de las actividades del sistema. Esta herramienta proporciona una pista independientemente verificable que permite la reconstrucción, revisión y evaluación de la secuencia de entornos y actividades que rodean o conducen a las operaciones, los procedimientos o eventos relacionados a una transacción desde el inicio hasta los resultados finales.

RIESGO[33]: 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.

SEGMENTACIÓN DE RED[34]: la segmentación de red separa componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta de sistemas que no lo hacen. Una segmentación de red adecuada puede reducir el alcance del entorno de los datos del titular de la tarjeta y, por lo tanto, reducir el alcance de la evaluación de las PCI DSS. Consulte la sección Segmentación de red en Requisitos de las DSS PCI y procedimientos de evaluación de seguridad para obtener información acerca del uso de segmentación de red. La segmentación de red no es un requisito de las PCI DSS. Consulte Componentes del sistema.

SEGURIDAD DE LA INFORMACIÓN[35]: protección de la información que garantiza la confidencialidad, integridad y disponibilidad.

SERVIDOR WEB[36]**:** computadora con un programa capaz de aceptar pedidos HTTP de clientes web y brindar respuestas HTTP (en general, páginas web).

---

[31] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 21
[32] Ibíd., p. 21
[33] Ibíd., p. 22
[34] Ibíd., p. 22
[35] Ibíd., p.23
[36] Ibíd., p.23

SERVIDOR[37]: computadora que presta servicios a otras computadoras, como el procesamiento de comunicaciones, almacenamiento de archivos y acceso a impresoras. Los servidores incluyen entre otros: web, base de datos, aplicaciones, autenticación, DNS, correo, proxy y protocolos NTP.

SISTEMA DE INFORMACIÓN[38]: conjunto específico de recursos de datos estructurados organizados para recolectar, procesar, mantener, usar, compartir, diseminar o disponer de la información.

SISTEMA OPERATIVO / OS[39]: software de un sistema de computadoras a cargo de compartir recursos informáticos y administrar y coordinar todas las actividades informáticas. Algunos ejemplos de sistemas operativos incluyen Microsoft Windows, Mac OS, Linux y Unix.

SOFTWARE MALICIOSO O MALWARE[40]: software desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema. Algunos ejemplos son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.

SSH[41]: abreviatura de “secure shell”. Conjunto de protocolos que proporcionan cifrado de servicios de red, como inicio de sesión remoto o transferencia remota de archivos.

SSL[42]: acrónimo de “secure sockets layer” (capa de conexión segura). Norma industrial establecida que cifra el canal entre un navegador web y un servidor web para garantizar la privacidad y confiabilidad de los datos transferidos por este canal.

TARJETAS DE PAGO[43]: en lo que concierne a las PCI DSS, toda tarjeta de pago o dispositivo que lleve el logotipo de los miembros fundadores de las PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide o Visa Inc.

---

[37] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 23

[38] Ibíd., p. 23

[39] Ibíd., p. 23

[40] Ibíd., p. 23

[41] Ibíd., p. 23

[42] Ibíd., p. 23

[43] Ibíd., p. 24

TELNET[44]: abreviatura de “telephone network protocol” (Protocolo de redes telefónicas). En general, se utiliza para proporcionar sesiones de inicio con líneas comandos orientadas al usuario para dispositivos de red. Las credenciales del usuario se transmiten en texto simple.

VPN[45]**:** acrónimo de “virtual prívate network” (red privada virtual) Una red informática donde algunas conexiones son circuitos virtuales dentro de redes más extensas, como Internet, en lugar de conexiones directas por medio de cables físicos. Cuando este es caso, los puntos finales de una red virtual se transmiten a través de una red mayor. Al contrario de una aplicación común, formada por comunicaciones seguras en la red pública, una red VPN puede presentar o no funciones de seguridad, como la autenticación y el cifrado de contenidos. Una VPN se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.

WEP[46]**:** acrónimo de “wired equivalent privacy” (privacidad equivalente por cable). Algoritmo débil utilizado en el cifrado de redes inalámbricas. Expertos de la industria han informado que la conexión WEP presenta varias debilidades tan serias que puede descifrarse en minutos utilizando herramientas de software comunes.

WLAN[47]: acrónimo de “wireless local área network” (red de área local inalámbrica). Red de área local que se conecta a dos o más computadoras o dispositivos sin cables.

[44] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs /PCI_DSS_v3_Glossary_ES-LA.pdf>. p. 25
[45] Ibíd., p. 26
[46] Ibíd., p. 26
[47] Ibíd., p. 26

RESUMEN

En el año [48]2006, un grupo de cinco entidades financieras, preocupado por el alto índice de fraudes con tarjetas de crédito, se reunió para crear un programa de seguridad de datos y fundaron un consejo denominado PCI Security Standards Council. Este grupo está conformado principalmente por American Express, Discover Financial Services, JCB International, MasterCard y VISA, este programa se aplica a todas las empresas que transmitan, procesen o almacenen datos de tarjetas de crédito o débito, no importa el tamaño de la misma, es decir que toda empresa que opere en el nicho de manejo de datos de tarjetahabientes está obligada a cumplir con este requerimiento para que sea reconocida por el PCI DSS como una empresa que provee los niveles de seguridad adecuados en los proceso que involucren información de tarjetahabientes, los niveles de seguridad propuestos por PCI DSS se obtienen aplicando controles y metodologías en las empresas, las metodologías básicamente se centran en tener un gobierno de seguridad bien estructurado, en donde existan unas políticas y lineamientos a seguir por todos los integrantes de la empresa, los controles también deben ir definidos en la política de seguridad de la empresa, algunos hacen parte de la cultura organizacional que debe implementar el gobierno de seguridad de la información, pero la gran mayoría son controles de tipo tecnológico, que implican despliegues de tecnologías a todos los niveles de la empresa, estos controles tecnológicos están dirigidos a:

- Blindar la red de la empresa contra posibles ataques.

- Evaluar las vulnerabilidades que puedan presentarse en la infraestructura.
- Controlar el tráfico generado por los usuarios finales desde el interior de la empresa.

- Controlar los posibles puntos en donde se puedan generar fugas de información referente a los datos de los tarjetahabientes.

- Mantener cifrado el almacenamiento y transmisión de datos de los tarjetahabientes.

Este requerimiento no es exclusivo de las grandes empresas del sector financiero, por el contrario aplica a las pequeñas y medianas empresas (PYMES) que son proveedores de las entidades financieras, es en este segmento de proveedores de servicios en donde se presenta la mayor dificultad para obtener la certificación PCI DSS debido a que el costo de adquisición de una plataforma tecnológica para

[48] BALCÁZAR, Priscila. Todo lo que necesita saber sobre PCI (Payment Card Industry Security Standards) y no se atrevía a preguntar. [En línea]. [consultado el 15 de junio de 2015]. Disponible en: http://www.magazcitum.com.mx/?p=59

asegurar el cumplimiento de los controles qué exige la certificación de la norma de seguridad de datos PCI DSS en su actual versión 3.0 puede llegar a ser muy elevado para una PYME, aun teniendo en cuenta que el costo puede variar dependiendo de las herramientas de hardware y software que cada PYME interesada en adquirir esta certificación elija, las herramientas que ofertan las empresas dedicadas al desarrollo de software y hardware especializado en seguridad informática es muy amplia y va desde soluciones simples hasta infraestructuras de gran complejidad. Aun así, para una PYME el hecho de adquirir la solución más sencilla implica una fuerte inversión monetaria, lo que puede llevar a la PYME a cuestionarse si vale la pena o no mantenerse en el segmento de empresas las que manejen datos de tarjeta habientes.

Debido a los elevados costos de implementación de los controles tecnológicos exigidos por PCI DSS V3.0, existe la necesidad de revisar opciones de implementación apoyándose en el software libre, esto con el fin de llevar la inversión económica a un nivel de inversión tolerable para una PYME.

ABSTRACT

In 2006, a group of five financial institutions, concerned about the high rate of credit card fraud, met to create a data security program and established a council called PCI Security Standards Council. This group consists mainly of American Express, Discover Financial Services, JCB International, MasterCard and VISA, this program applies to all companies that transmit, process or store card data credit or debit card, no matter the size of it, This means that any company operating in the niche handling cardholder data is required to comply with this requirement to be recognized by the PCI DSS as a company that provides appropriate levels of security in the process involving cardholder data, security levels proposed by PCI DSS are obtained by applying controls and methodologies in companies, methodologies basically focus on having a well structured security governance, where there are policies and guidelines to be followed by all members of the company, controls also must be defined in the security policy of the company, some are part of the organizational culture that the government must implement information security, but most controls are technological, technology deployments involving all levels of the company, these technological controls are aimed at:

- Shielding the company network against possible attacks.
- Assess the vulnerabilities that may arise in the infrastructure.
- Check the traffic generated by end users from within the company.
- Check the possible points where leaks can generate information regarding cardholder data.
- Keep storage encryption and transmission of cardholder data.

This requirement is not unique to large companies in the financial sector, by contrast applies to small and medium enterprises (SMEs) are suppliers of financial institutions, it is in this segment of service providers where the greatest difficulty arises for obtain PCI DSS certification because the acquisition cost of a technology platform to ensure compliance controls which requires certification of the standard data security PCI DSS in its current version 3.0 can be very high for PYME even considering that the cost can vary depending on hardware and software tools that each PYME interested in acquiring this certification choose the tools that offer companies engaged in software development and hardware that specializes in computer security is very broad and goes from simple solutions to very complex infrastructure. Yet the fact that PYME acquire the simplest solution involves a

strong monetary investment, which can lead to PYME to question whether it is worthwhile or not kept in the segment of companies that manage cardholder data.

Due to the high costs of implementation of technological controls required by PCI DSS V3.0, there is a need to review implementation options relying on free software, this in order to bring economic investment to a tolerable level of investment for a PYME.

INTRODUCCIÓN

La norma de seguridad de datos PCI DSS v3.0 "es un estándar que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito"[49].

Esta norma es concebida en 2006 por las principales compañías emisoras de tarjetas de crédito (Visa, Mastercard, American Express, JCB y Discover), debido a la cantidad de fraudes que se estaban presentando alrededor del mundo, por esta época "grandes compañías como TJX, Shell y Hannaford"[50], de acuerdo con "PrivacyRights.org"[51] en el 2005 más de 510 millones de registros con información sensible han sido violados, lo que motivo que las entidades emisoras establecieran la norma y que en la actualidad esta sea de cumplimiento obligatorio para todas las organizaciones que manipulen información de tarjetas de crédito.

Para el cumplimiento de esta norma, las organizaciones deben implementar una serie de herramientas de infraestructura tecnológica y procedimientos que permitan proteger la información sensible (Datos de Tarjeta Habientes). Para identificar que numerales de la norma requieren software, se debe realizar un cruce tecnología versus cumplimiento de la norma PCI- DSS v3.0, (véase el Anexo A).

Teniendo en cuenta los resultados del cruce tecnológico con los numerales de la norma.se concluye que se requieren herramientas tecnológicas como Firewall de Red, IPS, NTP, filtrado de contenido web, DLP, descubrimiento de datos de tarjeta, firewall de aplicación web, monitoreo de integridad de archivos, escáner de vulnerabilidades y cifrado de datos son necesarias para dar cumplimiento a los requisitos de la norma PCI DSS V 3.0 1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 2.2.3, 2.3, 3.4.1, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.5, 3.6.2, 3.6.3, 3.6.6, 4.1, 4.2, 5.1, 5.1.1, 5.2, 5.3, 6.6, 7.2, 7.2.1, 7.2.2, 7.2.3, 10.4, 10.4.1, 10.4.3, 10.5.5, 11.1, 11.2, 11.2.1, 11.3.3, 11.4, 11.5, 12.10.5.de la norma PCI DSS V 3.0.

---

[49] INTERNET SECURITY AUDITORS. Implantación y certificación en el estándar PCI DSS. [En línea]. < http://www.isecauditors.com/implantacion-pci-dss> [citado el 15 de Junio del 2015]

[50] CONSEJO DE ESTÁNDARES DE SEGURIDAD PCI O PCI. Oversight and History.[En línea]. [consultado el 15 de Junio del 2015], Disponible en: <http://www.focusonpci.com/ site/index.php/ pdf/About-PCI/pci-oversight-and-history.pdf>

[51] PRIVACY RIGTHS CLEARINHOUSE. Privacidad Derechos de la Cámara de Compensación (PRC) [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.privacyrights.org/>

La adquisición de las herramientas nombradas anteriormente demanda inversiones económicas que pueden llegar a ser bastante considerables para una PYME, costos que probablemente no podrían ser asumidos por una PYME. Martin Bradley y Alexander estudiantes graduados de maestría de Royal Holloway universidad de Londres, en su investigación realizada sobre "Payment Card Industry Data Security Standard (PCI DSS) – What it is and its impacton retail merchants (la industria de tarjetas de pago estándar de seguridad de datos (PCI DSS) - lo que es y su impacto en los comerciantes minoristas)"[52]. En el estudio que realizaron establecen que el costo de implementación en los comercios minoristas del Reino Unido de la norma PCI DSS, puede superar los 5 millones de Euros.

Estos valores hacen que el objetivo de certificarse para una PYME sea muy difícil de alcanzar, esto restringe la competitividad en este mercado y evita que empresas medianas o pequeñas puedan surgir, a causa de esta problemática.

Este proyecto se enfoca a las PYMES, y tiene como objetivo entregar una guía que especifique las mejoras prácticas para implementar tecnologías de seguridad informáticas enfocadas a dar cumplimiento a los controles tecnológicos exigidos por la norma PCI DSS v3.0.

La idea es que las PYMES puedan abordar el cumplimiento de los controles anteriormente nombrados mediante el uso herramientas de libre distribución, en los casos que aplique, es decir software no comercial, con un costo adquisición de cero, de esta forma las empresas solo incurrirán en costos de implementación y así se consigue hacer más viable la obtención de una certificación PCI DSS V3.0.

Para lograr el cometido descrito se tomará en cuenta la implementación de las siguientes herramientas de uso libre:

- Firewall de Red
- IPS
- NTP
- Filtrado de contenido
- DLP
- Descubrimiento de datos de tarjeta
- Firewall de aplicación
- Monitoreo de integridad de archivos
- Escáner de vulnerabilidades
- Antivirus
- Cifrado de datos

[52] BRADLEY Martin, DENT W. Alexander. Payment Card Industry Data Security Standard (PCI DSS) – What it is and its impact on retail merchants. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RHUL_Bradley_2010.pdf>

Para elaborar la guía es necesario realizar un análisis de los requisitos de la norma, y relacionarlos en los casos que aplique a una herramienta de seguridad informática, una vez realizado este análisis, es necesario proceder a investigar si existen o no opciones de software libre que satisfagan los requerimientos de la norma.

Una vez se obtengan estos resultados se elaborará la guía de implementación con el software libre seleccionado, para los casos en que aplique, es decir que podrán existir situaciones en donde la investigación demuestre que no existen herramientas de manejo libre para dar cumplimiento al requerimiento.

El resultado esperado con la elaboración de la guía, es permitir que las PYMES puedan implementar la norma de seguridad de datos PCI DSS v3.0 para los controles de la norma PCI DSS V 3.0. 1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 2.2.3, 2.3, 3.4.1, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.5, 3.6.2, 3.6.3, 3.6.6, 4.1, 4.2, 5.1, 5.1.1, 5.2, 5.3, 6.6, 7.2, 7.2.1, 7.2.2, 7.2.3, 10.4, 10.4.1, 10.4.3, 10.5.5, 11.1, 11.2, 11.2.1, 11.3.3, 11.4, 11.5, 12.10.5, utilizando software libre, lo cual debe verse reflejado en la disminución de uso de software comercial, y por ende reducir de manera considerable los costos de adquisición e implementación de software de seguridad informática.

1. FORMULACIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La norma internacional PCI DSS en su versión 3.0 vela por salvaguardar la seguridad de los datos de los tarjetahabientes, ya que día tras día los tarjetahabientes confían sus datos a empresas relacionadas con el comercio electrónico, bancos, tiendas online, pasarelas de pago entre otros, estos datos se convierten en un blanco de las organizaciones criminales, ya que al obtener dicha información les es posible realizar transacciones electrónicas y adquirir bienes y hacer retiros de efectivo, lo cual impacta la economía del tarjetahabiente y la reputación de la empresa vinculada en el compromiso de la información. Por este motivo se hace imprescindible regular el manejo de datos de tarjetahabientes y es ahí donde PCI DSS V3.0 se convierte en una herramienta que aporta gran valor a las empresas dedicadas a la transmisión, procesamiento o almacenamiento de datos de tarjetahabientes, el cumplimento de esta norma requiere de la implementación de controles tecnológicos y controles metodológicos, lo cual exige una fuerte inversión monetaria, es por este motivo que pensando en disminuir la inversión económica que implica la adquisición e implementación de tecnologías de seguridad informática para la protección de datos de tarjeta habientes, exigidas por la norma internacional PCI DSS V3.0 para una pequeña o mediana empresa, nace el siguiente interrogante:

¿Qué soluciones de software libre pueden ser implementadas en una PYME, para dar cumplimiento a los controles tecnológicos que exige la norma PCI DSS v3.0 y reducir costos asociados con la adquisición e implementación de software de seguridad informática?

1.2 JUSTIFICACIÓN

Los constantes ataques de los cibercriminales enfocados a abrir brechas de seguridad en las infraestructuras de las empresas dedicadas al manejo de datos de tarjetahabientes, hacen necesario la implementación de buenas prácticas y estándares generados por organizaciones dedicadas a combatir esta problemática, la norma internacional PCI DSS v3.0 fue [53]desarrollada para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

La adopción de las buenas prácticas propuestas en la PCI DSS v3.0 implican la implementación de controles tecnológicos y operativos al interior de las compañías que manejen datos de tarjetahabientes, los controles tecnológicos implican que las organizaciones deben dotarse de herramientas tecnológicas de seguridad

[53] PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 24

informática para proteger su infraestructura lo cual incluye la red LAN, la red inalámbrica, los activos de TI (Servidores y EndPoints), las bases de datos y las aplicaciones WEB, la implementación de herramientas tecnológicas de seguridad informática enfocadas a elevar la seguridad de los datos de los tarjetahabientes constituyen un pilar en los lineamientos propuestos por PCI DSS v3.0, de ahí que las compañías líderes en el mercado de la seguridad informáticas han dirigidos sus esfuerzos al desarrollo de herramientas que satisfacen esta necesidad.

Las propuestas son variadas pero en su gran mayoría estas soluciones llegan a alcanzar un alto costo, lo cual se convierte en una disyuntiva para las pequeñas y medianas empresas que por su deber ser, procesan, almacenan o transportan datos de tarjeta habientes, lo cual crea un cuestionamiento sobre la relación costo beneficio de obtener una certificación como la PCI DSS versión 3.0.[54]Un estudio realizado a principios de 2014 por el Ponemon Institute dirigido a 160 empresas de Estados Unidos, arrojo como resultado que el coste medio de implementar PCI DSS es de 3.5 millones de dólares, esta cifra puede convertirse en un obstáculo para una PYME que quiera buscar dicha certificación, por este motivo se hace necesario establecer mecanismos que permitan reducir los costos de adquisición e implementación de herramientas de seguridad informática que ayuden a cumplir los requisitos de la norma que exigen explícitamente el uso de soluciones tecnológicas para controlar y aminorar las posible brechas de seguridad, teniendo en cuenta esta situación es necesario explorar la posibilidad de dar cumplimiento a los controles tecnológicos exigidos por la norma PCI DSS versión 3.0 utilizando herramientas de libre distribución, las cuales permiten a las PYMES no incurrir en gastos de licenciamiento, lo que se ve directamente reflejado en la disminución de los costos de adopción de la norma PCI DSS versión 3.0.

1.3. OBJETIVOS

1.3.1 Objetivo general. Diseñar una guía de implementación de Firewall de Red, IPS, NTP, filtrado de contenido, DLP, Descubrimiento de datos de tarjeta en activos de TI, Firewall de aplicación, monitoreo de integridad de archivos, monitoreo de base de datos y cifrado de datos, que ayude a dar cumplimiento a los controles propuestos por la norma PCI DSS versión 3.0 que exigen la implementación de herramientas tecnológicas de seguridad informática, haciendo uso de software de libre distribución, y que permita reducir los costos de adopción de la norma por una PYME.

[54] FINANZAS Y BANCA. Hacia una estrategia consolidada para el cumplimiento de la normativa PCI DSS. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://www.finanzasybanca.com/index.php/hacia-una-estrategia-consolidada-para-el-cumplimiento-de-la-normativa-pci-dss.html>.

1.3.2 Objetivos específicos

- Identificar los requerimientos de la norma de seguridad de datos PCI DSS v3.0 en los cuales se establezca la necesidad de implementar tecnologías de seguridad informática para su cumplimiento.

- Identificar las herramientas libres ofrecidas por la comunidad de software libre que permitan el cumplimiento de los controles tecnológicos exigidos por la norma PCI DSS versión 3.0.

- Disminuir el costo final de un proceso de adopción de la norma PCI DSS versión 3.0 para una PYME, haciendo uso de herramientas tecnológicas de seguridad informática de libre distribución.

- Comparar herramientas de seguridad informática comerciales frente a herramientas de seguridad informática de libre distribución, que permitan dar cumplimiento a los requisitos de la norma PCI DSS versión 3.0 que exijan la implementación de estas tecnologías.

- Proponer la implementación de herramientas tecnológicas de seguridad informática de libre distribución para cumplir con los requisitos tecnológicos de la norma PCI DSS versión 3.0

- Identificar los requerimientos de la norma de seguridad de datos PCI DSS v3.0 que se pueden cumplir implementando soluciones de seguridad informática basadas en software libre.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

La seguridad informática nace de la necesidad de proteger los activos tecnológicos que alojan información valiosa para su dueño, con la masificación del uso de los ordenadores y su interconexión a través de internet el crimen puso su mira en estos, ya que no es necesario perpetrar el crimen de forma presencial, lo cual al parecer es lo más atractivo para los cyber delincuentes, ya que la mayoría de veces permanecen en el anonimato.

A continuación, se nombran algunos hechos relevantes en la historia que condujeron a la creación de normas para garantizar la seguridad de los activos tecnológicos.

Robert Tappan Morris. En noviembre de 1988, Robert Tappan Morris, también apodado RTM, creó un virus informático que infectó a cerca de seis mil máquinas Unix, haciéndolas tan lentas que quedaron inutilizables, causando millonarias pérdidas.

David L. Smith autor del famoso virus Melissa, que se propagó con éxito por correo electrónico en 1999. Fue condenado a prisión por causar daños por más de 80 millones de dólares.

Michael Calce quién el día de San Valentín de 2000, con apenas 15 años de edad, lanzó un ataque que afectó a eBay, Amazon y Yahoo!.

Sven Jaschan cierra la lista el creador del virus Sasser, quien fue detenido en mayo de 2004 tras una denuncia de sus vecinos que perseguían la recompensa incitada por la empresa Microsoft, ya que el virus afectaba directamente la estabilidad de Windows 2000, 2003 Server y Windows XP[55].

Los eventos anteriores obligaron a las compañías que prestan servicios financieros a crear políticas y procedimientos con el ánimo de ofrecer un mejor nivel de seguridad a sus usuarios, es así que en el año 2004 se reúnen las franquicias que mayor penetración tienen en el mercado de tarjetas de crédito, Visa y MasterCard y crean un conjunto de procesos y requisitos de la industria financiera y dan nacimiento al Estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago PCI DSS, (Payment Card Industry Data Security Standard), todo ello apoyado por los sistemas internacionales de pago con tarjetas.

[55] ALTONIVEL. Los 10 hackers más famosos del mundo. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.altonivel.com.mx/los-10-hackers-mas-famosos-del-mundo.html

En el mes de Septiembre del año 2006, como organización independiente y de la que forman parte todas las organizaciones que participan en la industria de pago con tarjetas, el Consejo de Seguridad de los Estándares de la Industria de las Tarjetas de Pago (PCI Security Standards Council), se hizo cargo de este conjunto de normas. El Consejo es ahora responsable de los estándares y de su desarrollo hasta la fecha[56]

2.2 MARCO TEÓRICO

Salvaguardar los datos de información sensible en una compañía, se ha convertido en todo un reto, ya que la adopción de metodologías de control en las empresas parte de una directriz institucional, la cual en algunos casos por arraigos culturales las empresas no están dispuestas a aceptar y se basan en métodos anticuados de manejo de la información sensible, apoyándose en la teoría de que así han venido trabajando los últimos años y de que las cosas hasta el momento les has salido bien, obviando por completo que las tecnologías de la información son de carácter dinámico y que en los últimos años se han convertido en el blanco predilectos de organizaciones al margen de la ley que buscan el lucro económico. La seguridad en la informática aparece de la mano con el desarrollo del concepto de delito informático, [57]"Los delitos Informáticos son todos aquellos actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de las computadoras y a través del mundo virtual de la internet", a raíz de la aparición del delito en los sistemas informáticos se crea la necesidad de combatirlo y salvaguardar la integridad de las infraestructuras.

Se inducen conceptos tales como integridad, confidencialidad y disponibilidad de la información, los cuales se aplican al manejo de la información en las empresas y hoy por hoy se convierten en los pilares del manejo seguro de la información, a fin de proteger la misma de manos inescrupulosas. Estos conceptos llegan a tener gran acogida en empresas del segmento de manejo de datos de tarjetahabientes, ya que esta información se puede prestar para realizar ilícitos con fines lucrativos, lo que convierte esta información es un preciado tesoro para los delincuentes, y se desata una guerra entre los dos bandos, los buenos que son los dueños de la información y quienes deben velar por la protección de la misma para garantizar y generar en sus clientes confianza en el manejo de la misma, esta información por lo general contiene datos como nombres completos, numero único de identidad, direcciones y teléfonos, y por el otro lado está el bando del mal, intentando

[56]VISA. Seguridad de los datos. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.visaeurope.es/visa-para-comercios/seguridad/seguridad-de-los-datos>
[57]CRIMESSYSTEMS. Cuál es la historia de los delitos informáticos. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://crimessystems.blogspot.es/>

apoderarse de esta información para perpetrar actos delictivos como estafas, extorciones y secuestros.

Es importante destacar la adopción de modelos de gobierno de seguridad de la información para aminorar la exposición al riesgo y el compromiso de la información y así prever posibles pérdidas monetarias, sanciones que en ocasiones pueden incluso repercutir en el cierre de una compañía y la perdida de reputación frente a los clientes.

2.3 MARCO REFERENCIAL

Toda compañía que maneje datos transaccionales financieros en donde se transmita, procese o almacene información de tarjetas de crédito, adquiere una gran responsabilidad en el manejo y resguardo de esta información por el alto grado de confidencialidad que deben garantizar a los usuarios sobre la misma, cuando la información se ve comprometida, no solamente conlleva a grandes pérdidas económicas, sino que adicionalmente pone en riesgo la reputación de la empresa, y por lo tanto en la mayoría de los casos la continuidad de un negocio, un ejemplo de esto se puede ver en empresas que fueron comprometidas con fugas de información y que tiempo después desaparecieron a causa de su pérdida de reputación.

Actualmente en [58]Colombia se registran pocas empresas certificadas PCI DSS, lo anterior debido a los elevados costos que supone su implementación, sin embargo se ha visto que la implementación de esta norma es una obligación para todas las empresas que operan con datos de tarjetas de crédito, sean entidades financieras, procesadores, comercios, desarrolladores de software o fabricantes. Esto a causa de la creciente delincuencia informática que ha causado innumerables fugas de información que exponen información confidencial de las personas, por eso es que muchas empresas como Visa Internacional, Master Card, American Express, exigen que sus clientes como entidades financieras, comercios, casas de desarrollo de software u otras entidades que realicen transacciones con tarjetas de crédito, deben estar certificadas para poder seguir vigentes en el mercado transaccional.

Es de gran importancia denotar que el hecho de que una empresa se encuentre certificada en la norma PCI-DSS no significa que sea invulnerable ya que la norma PCI DSS es apenas un conjunto mínimo de requisitos con el fin de proteger los datos del titular de tarjeta de crédito, un ejemplo de ello se puede evidenciar en lo

[58] INOCREDITO. Certifíquese en PCI. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.incocredito.com.co/index.php/para-establecimientos-comerciales/icomo afiliarse/ certifiquese-en-pci.html

sucedido a la compañía TARGET[59], una gran cadena de almacenes quien estando certificada PCI DSS, fue vulnerada causando una fuga de información de ciento diez millones de registros entre datos de tarjetas e información personal de los usuarios, lo que demuestra que siempre habrá una brecha o vulnerabilidad que la norma o la tecnología existente no puede cubrir, sin embargo esta certificación brinda un grado de confianza mayor en cuanto a que se está siguiendo un estándar y que la información está siendo tratada correctamente.

Las empresas grandes que cuentan con los recursos tecnológicos y financieros no tendrán mayor problema con la inversión necesaria para la implementación de la norma, sin embargo, que pasa con las pequeñas, medianas y micro empresas como cadenas de almacenes, casas de software o procesadores que están surgiendo, de esta forma surge el presente proyecto.

Algunas compañías han realizado sus propias guías de implementación para el cumplimiento de la norma PCI DSS utilizando su propio software, a continuación, se pueden observar algunos ejemplos:

- **Nombre proyecto: Guía de planeación para el cumplimiento del Estándar de seguridad de datos en la industria de tarjetas de pago[60]**

Autor: Microsoft

Es la Implementación de la Guía Microsoft para el cumplimiento del Estándar de seguridad de datos en la industria de tarjetas de pago, para la implementación Microsoft sugiere una gran cantidad de software licenciado en la cual se incluye Firewall, Antivirus, Firewall de Aplicación, Paquetes de Office con algunas extensiones adicionales de licenciamiento que permiten una funcionalidad de control en cuanto a fugas de información, estas son algunas entre 45 herramientas de software propuestas por Microsoft focalizado según La situación de cada organización, de cierta forma Microsoft propone adaptar algunas de sus herramientas para dar cumplimiento a la norma sin utilizar software de terceros.

Aunque la guía es bastante buena y concisa en las propuestas de software, y en intentar adaptarse a las diferentes situaciones de las organizaciones, es probable que la guía de Microsoft esté muy lejana para ser implementada por micro

[59] MUNDOFOX. Vicepresidente de Target inicia audiencia tras escándalo por perdida de información de clientes. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.noticiasmundofox.com/noticias/vicepresidente-de-target-inicia-audiencia-tras-escandalo-por-perdida-de-informacion-de

[60] TECHNET MICROSOFT. Guía de planeación para el cumplimiento del Estándar de seguridad de datos en la industria de tarjetas de pago. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://technet.microsoft.com/es-es/library/bb821241.aspx>

empresas debido a la cantidad de software licenciado requerido y su costo asociado.

- **Nombre Proyecto: Soluciones para necesidades empresariales PCI-DSS Compliance[61]**

Autor: Dell

Dell propone para el cumplimiento de la norma su soluciones SonicWALL[62] donde incorpora una gran cantidad de software para cifrado, redes, Virtualización y la gran mayoría de los puntos de la certificación, sin embargo es menos conciso en cuanto a la forma de implementación a diferencia de Microsoft.

Los proyectos de DELL y Microsoft presentan una similitud a lo propuesto en el proyecto actual, en cuanto a presentar una guía concisa que pueda facilitar la implementación de PCI-DSS. Sin embargo a diferencia de estos proyectos, la guía propuesta busca que las pequeñas, medianas y micro empresas que están iniciando e incursionando en nuevos mercados tengan la misma posibilidad de ser competitivas frente al mercado, al poder implementar la norma PCI-DSS 3.0 con software libre o con software que represente un costo relativamente bajo para una organización, se propondrá el mejor software free para la implementación de Firewall de red, IPS, NTP, Filtrado de Contenido, DLP, Descubrimiento de Datos de Tarjeta, Firewall de Aplicación y Cifrado de Datos que permita dar cumplimiento a la norma PCI – DSS 3.0 en los controles aplicables.

[61] DELL. Soluciones para necesidades empresariales PCI-DSS Compliance. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.sonicwall.com/es/es/solutions/Solutions-PCI-Compliance.html#tab=bestpractices>
[62] Ibíd.

3. DISEÑO METODOLÓGICO

El presente proyecto pretende examinar el mundo del software libre y correlacionarlo para su aplicación en el cumplimiento de la norma PCI DSS V 3.0, la utilización de software libre para dar cumplimiento a los controles tecnológicos de la normativa PCI DSS V 3.0 es poco conocida, si bien es cierto que unos pocos consultores en seguridad informática recomiendan el uso de software libre para cumplir con algunos controles de la norma, ninguno de ellos se ha tomado a la labor de identificar los controles puntuales que pueden cumplirse utilizando software libre ni tampoco las herramientas que ofrece la comunidad de software libre para centralizar este conocimiento y así disponerlo al servicio de las diversas compañías.

Es de aclarar que lo que busca esta investigación es implementar soluciones tecnológicas de seguridad informática ofertadas por la comunidad de software libre, las cuales sirvan de apoyo a una PYME para dar cumplimiento a los *controles* de la norma PCI DSS V 3.0, 1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 2.2.3, 2.3, 3.4.1, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.5, 3.6.2, 3.6.3, 3.6.6, 4.1, 4.2, 5.1, 5.1.1, 5.2, 5.3, 6.6, 7.2, 7.2.1, 7.2.2, 7.2.3, 10.4, 10.4.1, 10.4.3, 10.5.5, 11.1, 11.2, 11.2.1, 11.3.3, 11.4, 11.5, 12.10.5 de acuerdo a lo planteado en la norma PCI DSS en su versión 3.0.

Para lograr este objetivo se desarrollan los siguientes pasos:

- Verificar que herramientas tecnológicas se requieren para dar cumplimiento a los requisitos de la norma PCI DSS V 3.0 que obligatoriamente exigen la implementación de una herramienta tecnológica para su cumplimiento.

- Identificar los numerales de la norma que se pueden cubrir implementando herramientas tecnológicas de seguridad informática.

- Comparar las herramientas tecnológicas de uso libre frente a herramientas desarrolladas por casas comerciales, teniendo en cuenta parámetros puntuales exigidos por la norma PCI DSS V 3.0, para realizar esta comparación es necesario recurrir a las fuentes de información brindadas por los fabricantes (fichas técnicas) y por empresas dedicadas al análisis y clasificación de herramientas tecnológicas (Gartner), la idea es tomar la herramienta comercial líder del mercado y compararla contra la solución de software libre más destacada, es de aclarar que únicamente se compararán los módulos que homologuen conceptos de cara al cumplimiento de la norma PCI DSS V 3.0 a fin de que obtener un resultado objetivo y competitivo; es decir que las características adicionales que pueda ofrecer una herramienta tecnológica que no aporten para las exigencias de la

norma PCI DSS V 3.0 no serán tomadas en cuenta; pueden existir situación en las cuales solo uno o algunos módulos de una herramienta sean comparados.

– Concluir y recomendar el uso de una u otra herramienta a la luz del cumplimiento de los requisitos de la norma PCI DSS V 3,0 que exijan la implementación de herramientas tecnológicas; puede darse el caso en donde posterior al análisis se concluya que no existe una herramienta de software libre que cumpla a cabalidad con alguno de los requisitos de la norma PCI DSS V 3.0 que demandan la implementación de una solución tecnológica de seguridad informática, para tal caso se procederá a explicar el porqué del no cumplimiento.

4. ANÁLISIS DE HERRAMIENTAS

Para avanzar en la profundización de esta investigación es necesario analizar herramientas de tipo libre, versus herramientas comerciales, de esta forma se podrá establecer un contraste entre las ventajas y desventajas de las unas y las otras, de esta forma la persona que quiera implementar un proyecto de certificación PCI DSS en su versión 3.0, obtendrá una valioso material para contar con mejores criterios de decisión, las herramientas a tener en cuenta para dar cumplimiento a las exigencias de implementación tecnológica de la norma son:

- Firewall de Red
- IPS
- NTP
- Filtrado de contenido
- DLP
- Descubrimiento de datos de tarjeta
- Firewall de aplicación
- Monitoreo de integridad de archivos
- Escáner de vulnerabilidades
- Antivirus
- Cifrado de datos

Los numerales de la norma que exigen la implementación de herramientas tecnológicas son:

Numerales de la norma PCI DSS V 3.0, 1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 2.2.3, 2.3, 3.4.1, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.5, 3.6.2, 3.6.3, 3.6.6, 4.1, 4.2, 5.1, 5.1.1, 5.2, 5.3, 6.6, 7.2, 7.2.1, 7.2.2, 7.2.3, 10.4, 10.4.1, 10.4.3, 10.5.5, 11.1, 11.2, 11.2.1, 11.3.3, 11.4, 11.5, 12.10.5.

4.1 FIREWALL COMERCIAL VERSUS IP TABLES

Descripción: Un Firewall es un dispositivo de red cuya función es hacer filtrado de paquetes entre redes confiables (redes internas) y redes no confiables (redes externas)[63], de esta manera el firewall hace bloqueo de tráfico de red que no cumpla con los criterios de seguridad establecidos.

Toda compañía interesada en certificarse bajo la norma PCI DSS V 3.0 debe contar con un firewall con el fin de proteger la red de accesos no autorizados provenientes de redes no confiables tales como internet, conexiones de redes de

[63] PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 23

terceros (clientes, proveedores), conexiones de redes inalámbricas, con la implementación de un firewall es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[64]:

- *Numeral PCI DSS 1.1.4* Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.

- *Numeral PCI DSS 1.2* Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas.

- *Numeral PCI DSS 1.2.1* Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.

- *Numeral PCI DSS 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, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.

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

- *Numeral PCI DSS 1.3.1* Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.

- *Numeral PCI DSS 1.3.2* Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.

- *Numeral PCI DSS 1.3.3* No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.

- *Numeral PCI DSS 1.3.4* Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna).

[64] PCI SECURITY STANDARDS COUNCIL. Requisitos de las PCI PA-DSS y procedimientos de evaluación de seguridad, versión 3.0 Noviembre 2013. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf>

- *Numeral PCI DSS 1.3.5* No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.

- *Numeral PCI DSS 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").

- *Numeral PCI DSS 1.3.7* Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables

- *Numeral PCI DSS 1.3.8* No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

- *Numeral PCI DSS 7.2* Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente.

- *Numeral PCI DSS 7.2.1* Cobertura de todos los componentes del sistema.

- *Numeral PCI DSS 7.2.2* La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función.

- *Numeral PCI DSS 7.2.3* Configuración predeterminada de "negar todos".

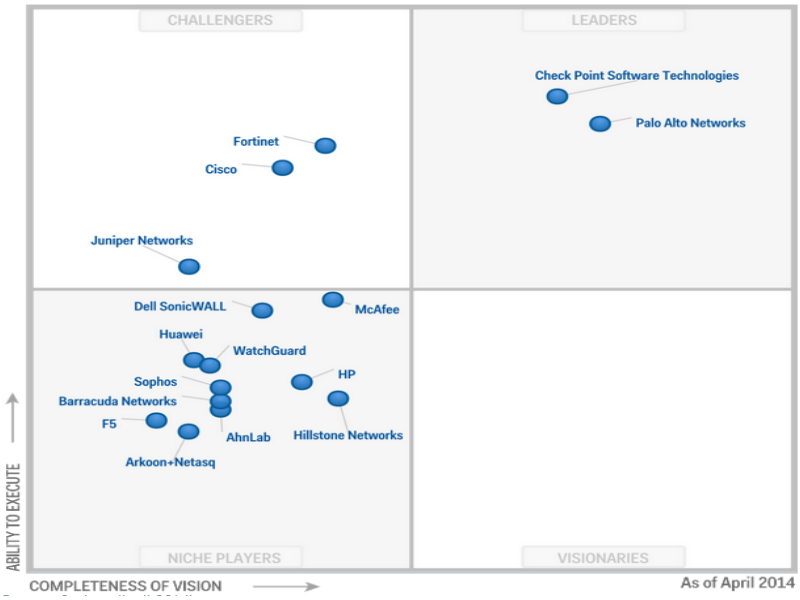
- *Numeral PCI DSS 2.10.5* Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

4.1.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [65]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, ver figura 1; el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho(NICHE

[65] GARTNERT, INC. investigación y análisis para las industrias. [En línea] [Consultado el 15 Junio de 2015] http://www.bnamericas.com/company-profile/es/gartner-inc-gartner.

PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre. (Ver figura 1)

Figura 1. Gartner Firewall



Fuente: GARTNER. Magic Quadrant for Web Application Firewalls. [En línea], [Consultado el 15 Junio de 2015]. Disponible en: https://www.gartner.com/doc/ 2770322/ magic-quadrant-web-application-firewalls

4.1.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar Firewall son las siguientes:

- Check Point (módulo de filtrado y contención)
- Fortinet (módulo de filtrado y contención)
- IP Tables

Se aclara que se hace referencia a módulos específicos de las marcas analizadas, porque las soluciones privadas adicional al módulo de firewall poseen otras características, que si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.1.1.2 Cuadro de comparación de Firewall´s comerciales y Firewall´s libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 1 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0, en el cuadro 1 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un firewall, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un firewall:

Cuadro 1. Comparación FIREWALL comercial vs FIREWALL libre frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	Checkpoint	Fortinet	Iptables
Numeral PCI DSS 1.1.4 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	√	√	√
Numeral PCI DSS 1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas.	√	√	√
Numeral PCI DSS 1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.	√	√	√
Numeral PCI DSS 1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta.	√	√	√
Numeral PCI DSS 1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.	√	√	√
Numeral PCI DSS 1.3.1 Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	√	√	√
Numeral PCI DSS 1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.	√	√	√
Numeral PCI DSS 1.3.3 No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.	√	√	√
Numeral PCI DSS 1.3.4 Implementar medidas antisuplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.	√	√	√
Numeral PCI DSS 1.3.5 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.	√	√	√
Numeral PCI DSS 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”).	√	√	√

Cuadro 1. (Continuación)

Requisito especifico	Comerciales		Software libre
	Checkpoint	Fortinet	Iptables
Numeral PCI DSS 1.3.7 Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables	√	√	√
Numeral PCI DSS 1.3.8 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.	√	√	√
Numeral PCI DSS 7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente.	√	√	√
Numeral PCI DSS 7.2.1 Cobertura de todos los componentes del sistema.	√	√	√
Numeral PCI DSS 7.2.2 La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función.	√	√	√
Numeral PCI DSS 7.2.3 Configuración predeterminada de "negar todos".	√	√	√
Numeral PCI DSS 12.10.5 Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.1.1.3 Cuadro de relación de funcionalidades de Firewall´s comerciales versus Firewall´s libres. En el cuadro 2 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 2 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un firewall, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 2**.** Relación de funcionalidades firewall comercial vs firewall libre

Funcionalidad	Comerciales		Software libre
	Checkpoint	Fortinet	Iptables
Análisis de consumo de tráfico de red	√	√	√
Inspección completa de paquetes full packetinspection	√	√	√
Consola de administración	√	√	√
Log de eventos	√	√	√
Traslación de direcciones de red NAT	√	√	√
Herramientas de solución de fallas	√	√	√
Soporte de VPN	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.1.1.4 Cuadro de relación de costos de Firewall´s comerciales versus Firewall´s libres

Cuadro 3. Relación Costos Firewall Comercial VS Firewall Libre

Descripción del costo	Comerciales		Software libre
	Checkpoint	Fortinet	Iptables
Licenciamiento de la herramienta	$47.175.000	$30.160.000	$0
Implementación	$28.774.200	$18.720.000	$5.000.000
Derechos de subscripción anual	$11.793.750	$7.540.000	$0
Soporte	$10.000.000	$10.000.000	$5.000.000
Costos de hardware	$0	$0	$11.236.000
TOTAL	$97.742.950	$66.420.000	$21.236.000

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.

A continuación, se explica el cuadro 3 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

  - CHECK POINT: El costo referenciado obedece al modelo firewall 4800.

  - FORTINET: El costo referenciado obedece al modelo firewall fortigate 800C.

o IP TABLES: Dado que IP TABLES es desarrollado por la casa [66]NET FILTER la cual se acoge a la filosofía de software de libre distribución, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o CHECK POINT: Los costos de implementación planteados por checkpoint son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo checkpoint, esto genera que los costos sean más elevados.

o FORTINET: Por tratarse de una marca que se encuentra ganando participación en el mercado, sus costos son más competitivos que los de las marcas ya posicionadas como líderes en el segmento.

o IP TABLES: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de tipo firewall se requieren alrededor de 50 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o CHECK POINT: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o FORTINET: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o IP TABLES: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [67]donaciones.

- Soporte:

[66] AYUSO NEIRA, Pablo. Licensing Information about net filter/iptables. [en línea], [consultado el 15 de Junio del 2015]. Disponible en; <http:// www.netfilter.org/licensing.html>

[67] FUNDACIÓN GNU. Donar hardware de computadora es también **útil** en ocasiones, [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://gnu.ist.utl.pt/help/donate.es.html#HowIndividualsCanDonate>

- CHECK POINT: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

- FORTINET: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

- IP TABLES: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000.

- Costos de hardware:

- CHECK POINT: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

- FORTINET: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

- IP TABLES: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante dimensionar de forma correcta la solución de firewall con el hardware adecuado, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

4.1.2 Conclusiones. La implementación de un firewall es obligatoria para dar cumplimiento a la norma PCI DSS, mediante esta implementación se consigue dar cumplimiento a 19 requisitos de la norma, esto indica la relevancia de contar con un firewall correctamente configurado, aquí es donde IP Tables se convierte en una excelente opción para una empresa que tiene recursos económicos limitados y quiere iniciar el proceso de certificación PCI DSS en su versión 3.0.

4.2 PROXY FILTRADO DE CONTENIDO COMERCIAL VERSUS SQUID

Un servidor proxy[68] es una aplicación utilizada como intermediario entre un explorador WEB e internet, el objetivo es centralizar conexiones HTTP, HTTPS y FTP, de esta forma las conexiones provenientes de clientes en redes internas se dirigen a redes externas, se envían a través de la dirección IP del proxy, es decir el o los servidores remotos identifican las conexiones originadas por los clientes a través de un único origen cuya dirección IP es la del proxy.

En adición a lo anterior los servidores proxy ayudan a mejorar el rendimiento en internet ya que almacenan una copia de las páginas WEB más utilizadas haciendo WEB cache, de esta forma cuando un explorador solicita una página WEB y esta previamente ha sido almacenada en el cache del proxy, el servidor proxy la proporciona inmediatamente sin necesidad de salir a internet en busca de la misma, lo que resulta en una percepción de navegación mucho más rápida.

Los servidores proxy también cuentan con funcionalidades de filtrado de contenido que ofrecen un mayor nivel de seguridad a la red. El filtrado de contenido evita que los usuarios naveguen en sitios categorizados de internet, ofreciendo niveles de seguridad y mayor productividad de los usuarios, unos ejemplos de categorías son: drogas, alcohol, deportes, pornografía, chat, video, recreación, hacking, películas, música, entre otros.

Un complemento a herramientas de seguridad tipo firewall es un proxy con filtrado de contenido, ya que comparten una función básica como lo es la protección de las redes internas de accesos no autorizados provenientes de redes poco confiables como internet, la implementación de proxy con filtrado de contenido ayuda a dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0.

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

- *Numeral PCI DSS 1.3.3* No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.

- *Numeral PCI DSS 1.3.8* No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

4.2.1 Comparación de herramientas libres contra herramientas privadas.

Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de

[68] MICROSOFT. ¿Qué es un servidor proxy? [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: http://windows.microsoft.com/es-co/windows-vista/what-is-a-proxy-server>

software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [69]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, ver figura 2; el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho (NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

Figura 2. Gartner Filtrado de contenido junio de 2014

Fuente GARTNER. Filtrado de contenido. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.gartner.com/technology/reprints.do?id=1-1VS13GJ&ct=140624&st=sb>

4.2.1.1 Herramientas evaluadas. Las herramientas a tener en cuenta para evaluar proxy con filtrado de contenido son las siguientes:

- WEB Sense (modulo de WEB filter & security)

[69] GARTNERT, INC. Op. Cit. p. 52

- Barracuda Networks (modulo WEB filter)
- SQUID

Se aclara que se hace referencia a módulos específicos de las marcas analizadas, porque las soluciones privadas complementan el módulo de filtrado WEB con características adicionales, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.2.1.2 Cuadro de comparación de Proxy´s comerciales y Proxy´s libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 4 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0, en el cuadro 4 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un proxy filtrado de contenido, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un proxy filtrado de contenido:

Cuadro 4. Comparación Proxy comercial vs Proxy libre frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	Web sense	Barracuda	Squid
Numeral PCI DSS 1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.	√	√	√
Numeral PCI DSS 1.3.3 No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.	√	√	√
Numeral PCI DSS 1.3.8 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.2.1.3 Cuadro de relación de funcionalidades de Proxy´s comerciales versus Proxy´s libres. En el cuadro 5 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 5 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un Proxy.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 5**.** Relación de funcionalidades Proxy comercial vs Proxy libre

Funcionalidad	Comerciales		Software libre
	Websense	Barracuda	Squid
Actualización de listas de categorías de filtrado	√	√	√
Consola de administración	√	√	√
Log de eventos	√	√	√
Generación de reportes	√	√	√
Herramientas de solución de fallas	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.2.1.4. Cuadro de relación de costos de Proxy filtrado de contenido comerciales versus Proxy filtrado de contenido libres

Cuadro 6. Relación de costos Proxy filtrado de contenido comercial vs Proxy filtrado de contenido libre

Descripción del costo	Proxy comerciales		Software libre
	Websense	Barracuda	Squid
Licenciamiento de la herramienta	$140'000.000	$27'750.000	$0
Implementación	$8'500.000	$6'200.000	$3'000.000
Derechos de subscripción anual	$28'000.000	$6'937.500	$0
Soporte	$10'000.000	$10'000.000	$5'000.000
Costos de hardware	$0	$0	$5'148.047
TOTAL	$186'500.000	$50'887.500	$13'148.047

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 6 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o WEBSENSE: El costo referenciado obedece al modelo appliance V5000.

o BARRACUDA: El costo referenciado obedece al modelo appliance 610.

o SQUID: Dado que el proxy SQUID pertenece al proyecto de software de libre distribución SQUID, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o WEBSENSE: Los costos de implementación planteados por WEBSENSE son relativamente elevados, debido al mercado donde tienen presencia, adicional los ingenieros que implementan o prestan soporte deben ser mano de obra certificada por el mismo WEBSENSE, esto genera que los costos se eleven.

o BARRACUDA: Por tratarse de una marca que se encuentra incursionando en el mercado, sus costos son más atractivos que los de las marcas ya posicionadas como líderes en el segmento.

o SQUID: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de tipo proxy

filtrado de contenido se requieren alrededor de 30 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o WEBSENSE: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, actualización de base de datos de categorización de sitios WEB y parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o BARRACUDA: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, actualización de base de datos de categorización de sitios WEB y parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o SQUID: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [70]donaciones, para el caso de actualización de base de datos de sitios WEB se puede hacer uso de listas como shallalist en el siguiente sitio: http://www.shallalist.de/categories.html.

- Soporte:

o WEBSENSE: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o BARRACUDA: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o SQUID: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000.

- Costos de hardware:

o WEBSENSE: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

[70] FUNDACIÓN GNU.. Op. Cit. p.49

o BARRACUDA: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o SQUID: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 1.8 GHZ
- Memoria RAM 8 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- 2 tarjetas de red

4.2.2 Conclusiones. Teniendo en cuenta los requisitos de la norma PCI que exigen la implementación de proxy con filtrado de contenido, SQUID se convierte en una alternativa funcional de menor costo para aquellas empresas pequeñas y medianas ya que como se puede observar SQUID cumple con las exigencias de los controles solicitados por PCI DSS 3.0.

4.3 IPS COMERCIAL VERSUS IPS SNORT

Un IPS o Sistema de prevención de intrusiones es un componente de seguridad muy importante para la protección de los sistemas en una red. Un IPS se basa en un IDS o sistema de detección de intrusión es con el componente añadido de tomar acciones, a menudo en tiempo real, con el fin de evitar una intrusión una vez sea detectada por el IDS[71].

El IPS de esta forma se convierte en una de las primeras barreras de seguridad para resguardar la red de ataques y amenazas, la implementación de herramientas de seguridad tipo IPS dan cumplimiento a los siguientes requisitos de la norma PCI DSS V 3.0.

- *Numeral PCI DSS 11.1* Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados.

[71]SANS INSTITUTE. A Design for Building an IPS Using Open Source Products. [En línea], [consultado el 15 de Junio del 2015]- Disponible en: <http://www.sans.org/reading-room/whitepapers/intrusion/design-building-ips-open-source-products-1662>

Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos.

Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.

- *Numeral PCI DSS 11.4* Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos.

Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.

4.3.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada.

Para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [72]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas. Esta empresa utiliza una metodología conocida como el cuadrante mágico. (ver figura 3);

El cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho(NICHE PLAYERS).Para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende, va totalmente en contra de la filosofía del software libre.

[72]GARTNERT, INC. Op. Cit. p. 52

Figura 3. Gartner IPS publicado Diciembre de 2014

Fuente: GARTNER. Magic Quadrant for Web Application Firewalls. [En línea]. [consultado el 15 de Junio del 2015]- Disponible en <http://www.gartner.com/technology /reprints.do?id=1-26MDU0D&ct=141230&st=sb>

4.3.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar IPS son las siguientes:

- CISCO (FirePower 7000)
- HEWLETT PACKARD (TIPPING POINT S2600NX)
- SNORT IPS

Se aclara que se hace referencia a módulos específicos de las marcas analizadas, porque las soluciones privadas complementan el módulo de IPS con características adicionales, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.3.1.2. Cuadro de comparación de IPS comerciales versus IPS libre frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 7 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0.

En el cuadro 7 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un sistema de prevención de intrusos IPS.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un sistema de prevención de intrusos IPS:

Cuadro 7**.** Comparación IPS comercial vs IPS libre frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	Cisco	Hewlett packard	Snort
Numeral PCI DSS 11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados. Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos.	√	√	√
Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.			
Numeral PCI DSS 11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.3.1.3 Cuadro de relación de funcionalidades de IPS comerciales versus IPS libre. En el cuadro 8 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla. Las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra.

En el cuadro 8 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un IPS.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 8. Relación de funcionalidades IPS comercial vs IPS libre

Funcionalidad	**IPS comerciales**		**Software libre**
	Cisco	**Hewlett packard**	**Snort**
Actualización de listas de categorías de filtrado	√	√	√
Consola de administración	√	√	√
Log de eventos	√	√	√
Generación de reportes	√	√	√
Herramientas de solución de fallas	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

Cuadro 9. Relación costos IPS comercial VS IPS libre

Descripción del costo	**IPS comerciales**		**Software libre**
	Cisco	**Hewlett packard**	**Snort**
Licenciamiento de la herramienta	$154’182.500	$112’000.000	$0
Implementación	$25’710.000	$17’300.000	$3’000.000
Derechos de subscripción anual	$18’810.000	$15’700.000	$0
Soporte	$10’000.000	$10’000.000	$5’000.000
Costos de hardware	$0	$0	$5’148.047
TOTAL	$208’702.500	$155’000.000	$13’148.047

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 9 de costos:(todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o CISCO FIRE POWER: El costo referenciado obedece al modelo 7050.

o HEWLETT PACKARD: El costo referenciado obedece al modelo TIPPING POINT S2600NX.

o SNORT: Dado que el IPS SNORT pertenece al proyecto de software de libre distribución SNORT, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o CISCO FIRE POWER: Los costos de implementación planteados por CISCO son relativamente elevados, debido al mercado donde tienen presencia, adicional los ingenieros que implementan o prestan soporte deben ser mano de obra certificada por el mismo CISCO, esto genera que los costos se eleven.

o HEWLETT PACKARD: Por tratarse de una herramienta de seguridad de esta compañía que se encuentra incursionando en el mercado, sus costos son más atractivos que los de las marcas ya posicionadas como líderes en el segmento.

o SNORT: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de tipo IPS se requieren alrededor de 30 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o CISCO: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, y parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o HEWLETT PACKARD: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o SNORT: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [73]donaciones.

[73] FUNDACIÓN GNU. Op. Cit. p. 56.

- Soporte:

o CISCO: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o HEWLETT PACKARD: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o SNORT: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000.

- Costos de hardware:

o CISCO: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o HEWLETT PACKARD: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o SNORT: Como costo asociado a la implementación de esta herramienta de seguridad es necesario adquirir un servidor que provea características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de hardware exigido, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

4.3.2 Conclusiones. Aunque los requisitos de la norma PCI DSS 3.0 que hacen mención a la implementación de herramientas de seguridad tipo IPS se describen en los numerales de la …norma 11.1 y 11.4…, no se deben menospreciar el apoyo que estos brindan a la seguridad. Los IPS ofrecen niveles de seguridad adicionales a los niveles de seguridad provistos por otro tipo de herramientas de seguridad, de esta forma no basta con la implementación de firewalls tradicionales

que filtran accesos a determinados servicios o puertos TCP/UDP, los IPS por su parte van más allá e inspeccionan de una forma más profunda las peticiones de conexiones de red a las aplicaciones convirtiéndose en un importante punto de control adicional.

Por lo anterior el IPS SNORT ofrece sus bondades con una mezcla de seguridad y costo favorable en la implementación de un sistema de prevención de intrusos IPS, de esta forma de nuevo haciendo uso de herramientas que pertenecen a la comunidad libre se convierten en una excelente opción para una empresa que tiene recursos económicos limitados y tienen la necesidad ya sea por exigencia de sus clientes o por ir en busca de oportunidades de entrar en el nicho de mercado financiero requiere iniciar el proceso de certificación PCI DSS en su versión 3.0.

4.4 WAF COMERCIAL VERSUS WAF MOD SECURITY

Un WAF o web application firewall o firewall de aplicaciones Web, es un dispositivo el cual realiza funciones de filtrado en el que se aplica un conjunto de reglas con el fin de hacer validaciones entre conexiones de clientes lanzadas al servidor HTTP. En general, estas reglas cubren ataques comunes tales como cross-site scripting (XSS) y SQL injection. Mediante la personalización de las reglas para su aplicación, muchos ataques pueden ser identificados y bloqueados. El esfuerzo para llevar a cabo esta personalización puede ser significativo y debe ser mantenido cada vez que se modifica la aplicación[74]. La implementación de herramientas de seguridad WAF ofrece cumplimiento a los siguientes requisitos de la norma PCI DSS V 3.0.

- *Numeral PCI DSS 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 con 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.

  - Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.

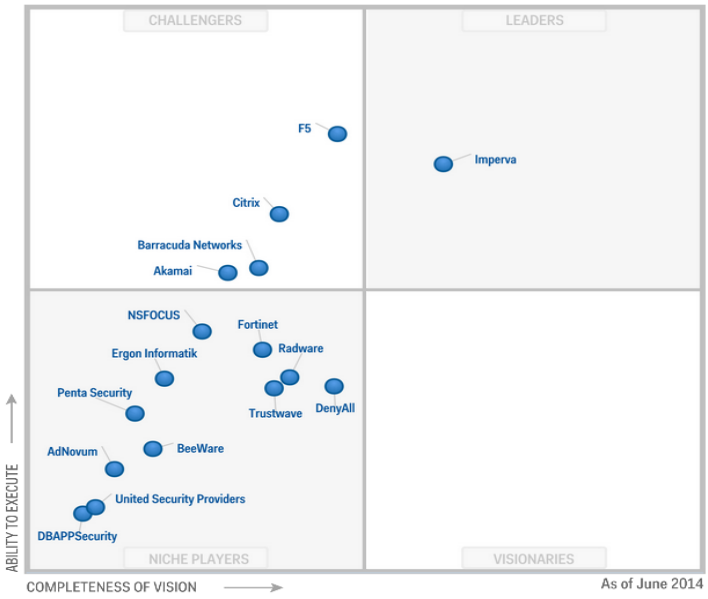
[74] OWASP.WEB. application firewall. [en línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.owasp.org/index.php/Web_Application_Firewall>[citado el 15 de Junio del 2015]

- *Numeral PCI DSS 12.10.5*Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

4.4.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada. Para las herramientas privadas se tomará la calificación dada por la empresa estadounidense Gartnert[75] dedicada a la consultoría y la investigación de tecnologías informáticas. Esta empresa utiliza una metodología conocida como el cuadrante mágico, (ver figura 4).

El cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho (NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

Figura 4. Gartner WAF publicado Junio de 2014



Fuente: GARTNER. Magic Quadrant for Web Application Firewalls. [En línea]. [consultado el 15 de Junio del 2015]- Disponible en <http://www.gartner.com/technology /reprints.do?id=1-26MDU0D&ct=141230&st=sb>

[75] GARTNER, Op. Cit. p. 58.

4.4.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar WAF son las siguientes:

- IMPERVA
- F5 (Módulo WAF)
- MOD SECURITY

Se aclara que se hace referencia a módulos específicos de las marcas analizadas, porque las soluciones privadas complementan el módulo WAF con características adicionales, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.4.1.2 Cuadro de comparación de WAF comerciales y WAF libre frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 10 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0.

En el cuadro 10 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un Web Application Firewall.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta los requisitos de la norma PCI DSS 3.0 en los cuales se requiere la implementación de un Web Application Firewall (WAF):

Cuadro 10. Comparación WAF al vs WAF libre frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	Imperva	F5	Modsecurity
Numeral PCI DSS 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 con 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. Nota: Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2. • Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.	√	√	√
Numeral PCI DSS 12.10.5 Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.4.1.3 Cuadro de relación de funcionalidades WAF comerciales versus WAF libre. En el cuadro 11 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra.

En el cuadro 11 se utilizan tres columnas, la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un WAF, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 11**.** Relación de funcionalidades WAF comercial vs WAF libre

Funcionalidad	WAF comerciales		Software libre
	Imperva	F5	Modsecuruty
Actualización de firmas de detección ataques	√	√	√
Consola de administración	√	√	√
Log de eventos	√	√	√
Generación de reportes	√	√	√
Herramientas de solución de fallas	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.4.1.4 Cuadro de relación de costos de WAF comerciales versus WAF libre

Cuadro 12. Relación costos WAF comercial vs WAF libre

Descripción del costo	WAF comerciales		Software libre
	Imperva	F5	Modsecurity
Licenciamiento de la herramienta	$145’000.000	$ 124’849.140	$0
Implementación	$17’324.000	$ 14’214.550	$4’000.000
Derechos de subscripción anual	$27’000.000	$29’382.311	$0
Soporte	$10’000.000	$10’000.000	$5’000.000
Costos de hardware	$0	$0	$5’148.047
TOTAL	$199’324.000	$178’446.001	$14’148.047

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 12 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

  - IMPERVA X2510: El costo referenciado obedece al modelo X2510.

  - F5: El costo referenciado obedece al modelo BIG IP 4000.

  - MOD SECURITY: Dado que el WAF MOD SECURITY pertenece al proyecto de software de libre distribución MODSECURITY, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o IMPERVA X2510: Los costos de implementación planteados por IMPERVA son relativamente elevados, debido al mercado exclusivo donde tienen presencia, adicional los ingenieros que implementan o prestan soporte deben ser mano de obra certificada en las herramientas IMPERVA, el contar con personal certificado hace que los costos de implementación sean elevados.

o F5 BIG IP 4000: Por tratarse de una herramienta de seguridad de esta compañía que se encuentra incursionando en el mercado, sus costos son más atractivos que los de las marcas ya posicionadas como líderes en el segmento.

o MOD SECURITY: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100. 000.oo. y para implementar una solución de tipo IPS se requieren alrededor de 50 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o IMPERVA: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, y parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o F5: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software, parches de seguridad, normalmente esta suscripción equivale a un rango entre un 20% y un 25% del costo de adquisición.

o MOD SECURITY: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [76]donaciones.

- Soporte:

o IMPERVA: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o F5: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de$ 200.000.

[76] FUNDACIÓN GNU. Op. Cit. p. 62

o MOD SECURITY: Se calculó una bolsa de 50 horas para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100. 000.oo.

- Costos de hardware:

o IMPERVA: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o F5: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o MOD SECURITY: Como costo asociado a la implementación WAF MOD SECURITY es necesario adquirir un servidor que provea características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de hardware exigido, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

4.4.2 Conclusiones. Los firewall de aplicación WEB son herramientas de seguridad necesarias en la protección de ambientes WEB, este tipo de herramientas se adhieren como módulo adicional de la aplicación brindando niveles de seguridad para protegerla de ataques de tipo cross-site scripting (XSS) y SQL injection, PCI DSS versión 3.0 en su requisito 6.6 brinda dos opciones para dar cumplimiento a este requisito, el primero se trata de evaluaciones de seguridad a la aplicación WEB que deben realizarse mínimo una vez al año o cada vez que se realizan cambios sobre la aplicación WEB, la segunda opción se trata de la implementación de herramientas firewall de aplicación WEB o WAF, dado que la aplicaciones WEB frecuentemente deben ser actualizadas ya sea por campañas o solicitud de clientes la primera opción puede tornarse costosa y no ofrece el nivel de seguridad necesario para portales transaccionales financieros, por otra parte la segunda opción con la implementación de un WAF ofrece niveles de seguridad constantes que deben ser actualizadas sus políticas con los cambios realizados sobre el servidor WEB con el fin de estar de esta forma sincronizado con la aplicación WEB.

Para una PIME no resulta fácil invertir en este tipo de herramientas de seguridad comerciales que son bastante costosas, la opción de una herramienta libre que pueda ofrecer niveles mínimos de seguridad resulta muy atractiva, por lo anterior el firewall de aplicación WEB MOD SECURITY es una opción favorable en costo beneficio para dar cumplimiento al requisito 6.6 y 12.10.5 de la norma PCI DSS V 3.0.

4.5 ANTIVIRUS COMERCIAL VERSUS ANTIVIRUS LIBRE

Los antivirus son programas cuyo objetivo es detectar, eliminar y evitar la activación de malware[77]. La aparición de nuevas tecnologías (Sistemas operativos, internet, etc.…), ha causado que los antivirus tengan que evolucionar, no solo detectándolos si no que adicional sean desarrollados para combatirlos.

Así cómo evoluciona la tecnología, también evolucionan los malware, por eso es necesario que un antivirus esté siempre actualizado. Es de tener en cuenta que el Antivirus nunca garantizara una protección del 100% su efectividad es relativa, ya que a diario salen nuevas amenazas y se generan nuevos tipos de malware, por lo cual nunca existirá una base de datos completa de malware existente que garantice una protección completa e irrompible.

En el mercado existen muchas soluciones que permiten la protección de los sistemas, cada uno de estos ofrecen funcionalidades similares.

La norma PCI-DSS, exige proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente, por lo cual la implementación de un antivirus se vuelve obligatorio para el cumplimiento de la norma, con la implementación de un antivirus es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[78]:

- *Numeral PCI DSS 5.1* Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).

- *Numeral PCI DSS 5.1.1* Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.
- *Numeral PCI DSS 5.2* Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente:

[77] MICROSOFT. Op. Cit. p. 58
[78] PCI SECURITY STANDARDS COUNCIL. Requisitos de las PCI PA-DSS y procedimientos de evaluación de seguridad, versión 3.0 Noviembre 2013. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: https:// www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

- Estén actualizados.

- Ejecuten análisis periódicos.

- Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.

- *Numeral PCI DSS 5.3* Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado.

Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus."

4.5.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [79]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, ver figura 5; el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho (NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

[79] GARTNERT, INC. Op. Cit. p. 66.

Figura 5. Gartner Antivirus publicado Diciembre de 2014

Fuente: GARTNER. Magic Quadrant for Web Application Firewalls. [En línea]. [consultado el 15 de Junio del 2015]- Disponible en <http://www.gartner.com/technology /reprints.do?id=1-26MDU0D&ct=141230&st=sb>

4.5.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar Firewall son las siguientes:

- McAfee(EndpointProtectionEssentialfor SMB[80])
- Cómodo(Endpoint Security Manager[81])
- ClamAV[82]

[80] MCAFEE.ENDPOINT Protection Essential for SMB. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.shopmcafee.com.co/store/mfesmb/es_MX/ pd/ThemeID. 36633 000/productID.306911700/categoryID.66300000>

[81] COMODO. COMODO. Endpoint Security Manager (ESM). [En línea], [consultado el 15 de Junio del 2015]. Disponible en: https://www.comodo.com/business-enterprise/endpoint-protection/endpoint-security-manager.php

[82] CLAMAV. CLAM. AntiVirus 0.98. User Manual. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <https://github.com/vrtadmin/clamav-faq/raw/master/manual/clamdoc.pdf>

Se hace claridad que se referencian módulos específicos de las marcas analizadas, porque las soluciones privadas adicional al módulo de anti-virus poseen otras características, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.5.1.2. Comparativo Antivirus comerciales y antivirus free frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 13 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0[83].

En el cuadro 13 se utilizan tres columnas principales. La primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un Antivirus.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un Antivirus:

[83]PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 71

Cuadro 13. Comparación antivirus comercial vs antivirus libre frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	McAfee	Comodo	Clamav
Numeral PCI DSS 5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).	√	√	√
Numeral PCI DSS 5.1.1 Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.	√	√	√
Numeral PCI DSS 5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: • Estén actualizados. • Ejecuten análisis periódicos. • Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.	√	√	
Numeral PCI DSS 5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado. Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus.	√	√	

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.5.1.3 Relación de funcionalidades de antivirus comerciales versus antivirus libres. En el cuadro 14 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 14 se utilizan tres columnas principales.

La primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un Antivirus, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software

libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 14**.** Relación de funcionalidades antivirus comercial vs antivirus libre

Funcionalidad	Comerciales		Software libre
	McAfee	Cómodo	Clamav
Actualización automática de firmas y componentes	√	√	√
Ejecución de análisis periódicos programados	√	√	√
Log de Eventos (pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses)	√	√	
Consola De Administración	√	√	
Solución antimalware activa(Escaneo en tiempo real)	√	√	
Detección y Eliminación de Malware conocido	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.5.1.4 Cuadro de relación de costos de antivirus comerciales versus antivirus libres (Ver cuadro 15)

Cuadro 15. Relación costos Antivirus comercial vs Antivirus libre

Descripción del costo	Comerciales		Software libre
	McAfee	Cómodo	Clamav
Licencia herramienta por estación 1 año (Valor variable según TRM).	$500.349 (10 licencias)	$916.500(mínimo 10 para consola)	$0
Licenciamiento por estación adicional	$50.034	$91.650	$0
Implementación.	$2’000.000	$2’000.000	$500.000
Renovación por licencia.	$125.087 (10 licencias)	$229.125 (10 licencias)	0
Soporte.	Incluido con la compra de licencias	Incluido con la compra de licencias	$0
Costos de Hardware	$4’599.990	$4’599.990	$0
TOTAL	$7’222.426	$7’745.615	$1’500.000

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 15 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o MCAFEE: El costo de referencia corresponde a la solución Endpoint Protection Essential for SMB, en el cuadro de costos se incluyen licenciamiento para 10 estaciones.

o CÓMODO: El costo de referencia corresponde a la solución End point Security Manager en el cuadro de costos se incluyen licenciamiento para 10 estaciones.

o CLAMAV: Dado a que la aplicación de libre, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o MCAFEE: Los costos de implementación corresponden a instalación de la aplicación y parametrización de la misma por parte del personal de TI, no requiere personal especializado.

o CÓMODO: Los costos de implementación corresponden a instalación de la aplicación y parametrización de la misma por parte del personal de TI, no requiere personal especializado.

o CLAMAV: Los costos de implementación del Software son bajos debido a que no tiene consola de administración, por lo cual su costo de implementación corresponde a la mano de obra de instalación de los agentes en cada equipo.

- Derechos de suscripción anual:

o MCAFEE: Se debe realizar renovación de licenciamiento para tener derechos a actualizar la base de datos de malware con las últimas amenazas detectadas por el fabricante, de igual forma para tener derecho a actualización y soporte de componentes del mismo, El valor de renovación es variante dependiendo del tiempo de renovación a contratar y la cantidad de licencias a renovar, el costo del cuadro corresponde a la renovación por un año de 10 licencias.

o CÓMODO: Se debe realizar renovación de licenciamiento para tener derechos a actualizar la base de datos de malware con las últimas amenazas detectadas por el fabricante, de igual forma para tener derecho a actualización y soporte de componentes del mismo, El valor de renovación es variante dependiendo del tiempo de renovación a contratar y la cantidad de licencias a renovar, el costo del cuadro corresponde a la renovación por un año de 10 licencias.

o CLAMAV: No es necesario pagar renovación para tener derechos de actualización de base de datos de malware, de igual forma tampoco para los nuevos componentes del antivirus, sin embargo, si es necesario estar pendiente de las nuevas versiones en la página del fabricante, ya que los antivirus de uso libre por lo general no actualizan sus componentes de forma automática, únicamente su base de datos de malware se actualiza de forma automática cada dado tiempo.

- Soporte:

o MACAFEE: El derecho a soportes se incluye dentro del mismo valor de licenciamiento como un servicio postventa, por lo cual no se requiere pagos adicionales, en el caso de este fabricante el soporte incluido es telefónico 7X24, sin embargo, también se puede realizar contratos de bolsas de horas presenciales para un soportes más formal y personalizado por un valor adicional.

o CÓMODO: El derecho a soportes se incluye dentro del mismo valor de licenciamiento como un servicio postventa, por lo cual no se requiere pagos adicionales, en el caso de este fabricante el soporte incluido es telefónico 7X24. debido a que este fabricante no tiene casi presencia en Latino América, la contratación o adquisición de una bolsa de horas presenciales podría tener costos elevados.

o CLAMAV: Por ser una herramienta libre no es necesario realizar pago de soporte, este es gratuito en la página del fabricante y es basado en correo electrónicos y Foros de ayuda.

- Costos de hardware:

o McAfee: Es necesario la adquisición de un servidor que cumpla con las especificaciones de hardware y Software (Sistema Operativo) para la instalación de la consola de administración para la gestión centralizada de estaciones.

Se plantea adquisición de servidor con las siguientes características para un óptimo funcionamiento.

- Memoria UDIMM de 8 GB
- Disco duro cableado de 1 TB
- Procesador Intel® Xeon® E3-1220 v3, 3,1 GHz
- Sistema Operativo Windows Server® 2012 R2, Foundation Edition

o CÓMODO: Es necesario la adquisición de un servidor que cumpla con las especificaciones de hardware y Software (Sistema Operativo) para la instalación de la consola de administración para la gestión centralizada de estaciones.

- Memoria UDIMM de 8 GB
- Disco duro cableado de 1 TB
- Procesador Intel® Xeon® E3-1220 v3, 3,1 GHz
- Sistema Operativo Windows Server® 2012 R2

o CLAMAV: Por no tener consola de administración centralizada, no requiere inversión de Hardware.

4.5.2 Conclusiones. Los antivirus comerciales versus los antivirus libres tienen una ventaja clara, que les permite cumplir con todos los requisitos concernientes a la implementación de un antivirus exigidos por la norma PCI DSS V 3.0, estos son la Consola de Administración para el monitoreo y gestión de las estaciones de trabajo, y el análisis activo o en tiempo real de las estaciones, aspectos que en la mayoría de los casos lamentablemente no pueden ser cumplidos por ninguno de los antivirus libre, la selección de ClamAV se realizó teniendo en cuenta su versatilidad en la posibilidad de instalarlo sobre cualquier Sistema Operativo; sin embargo debido a que no cumple con los requisitos de la norma se descarta totalmente la instalación de un antivirus libre para el cumplimiento de esta norma.

Como recomendación se observa que las grandes compañías líderes de Antivirus, han comenzado a liberar soluciones de antivirus específicas para pequeñas y medianas empresas muy competitivas, que son asequibles en cuanto a precio y que brindan una gran garantía, por lo cual es recomendable antes de tomar cualquier decisión por un antivirus de gama media, entrar a analizar estas opciones ofrecidas por los lideres, ya que no necesariamente un antivirus menos reconocido va a ser más asequible o barato que los ofrecidos por las grandes fabricantes como se pudo observar en el análisis de costos.

4.6 SERVIDOR NTP COMERCIAL VERSUS SERVIDOR NTP LIBRE

NTP (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123[84].

Está diseñado para resistir los efectos de la latencia variable. Utiliza un sistema de jerarquía de estratos de reloj, en donde los sistemas de estrato 1 están sincronizados con un reloj externo tal como un reloj GPS a algún reloj atómico. Los sistemas de estrato 2 de NTP derivan su tiempo de uno o más de los sistemas de estrato 1, y así consecutivamente hasta el estrato 4. NTP proporciona los

[84] WIKIPEDIA. Network Time Protocol. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: http://es.wikipedia.org/wiki/Network_Time_Protocol.

mecanismos para sincronizar la hora y coordinar la distribución del tiempo en un sistema.

La norma PCI-DSS, exige la utilización de tecnología de sincronización, sincronizar todos los tiempos y relojes críticos, por lo cual la implementación de un servidor NTP se vuelve obligatorio para el cumplimiento de la norma, con la implementación de un servidor NTP es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[85]:

- *Numeral PCI DSS 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.

Nota: Un ejemplo de tecnología de sincronización es el NTP (protocolo de tiempo de red).

- *Numeral PCI DSS 10.4.1* Los sistemas críticos tienen un horario uniforme y correcto.

- *Numeral PCI DSS 10.4.3* Los parámetros de la hora se reciben de fuentes aceptadas por la industria.

4.6.1 Comparación de herramientas libres contra herramientas privadas. Para esta implementación se tiene la facilidad que hay muchos servidores en internet que ofrecen el servicio de sincronización NTP que son confiables (es decir, aceptadas por la industria) y que son gratis un ejemplo de estos es la Superintendencia de Industria y Comercio, en cuanto a la implementación del servidor, se puede hacer con un servidor Linux con sistema operativo CentOS, Fedora, Open SUSE o Red Hat, esta última opción no es completamente gratis, es necesario pagar una suscripción para soporte y mantenimiento, sin embargo es accesible y provee grandes beneficios en cuanto a actualizaciones de seguridad y el soporte prestado por personal especializado.

Estas soluciones son todas Linux por lo que tienen funcionalidades muy similares, adicional a esto Red Hat apoya el proyecto Fedora y CentOS, por lo cual son casi iguales y muy estables para servidores, por ser todos sistemas operativos libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende, va totalmente en contra de la filosofía del software libre.

[85]PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 74

4.6.1.1 Herramientas evaluadas. Ya que el servicio de sincronización con un servidor NTP confiable es gratuito y no es necesario realizar ningún pago, se evaluarán las herramientas (Sistemas Operativos) con los cuales se puede implementar el servidor NTP. Las herramientas que se van a tener en cuenta para evaluar la implementación son las siguientes:

- Linux RED HAT
- Linux CentOS
- Windows Server 2012

4.6.1.2 Comparación de implementación servidor de sincronización NTP comercial y servidor de sincronización NTP libre frente al cumplimiento de la norma PCI DSS V 3.0. El servicio de sincronización NTP aceptable por la industria, es ofrecido por múltiples organizaciones y empresas de forma gratuita, por lo cual no se hace necesario un cuadro de comparación ya que todos cumplirán con los numerales de la norma PCI DSS V 3.0 exigidos para este control.

4.6.1.3 Relación de funcionalidades de implementación servidor de sincronización NTP comercial versus implementación servidor de sincronización NTP libre. Las funciones de la sincronización de NTP para el cumplimiento de la norma van de acuerdo a la forma de implementación del servidor y la configuración de la infraestructura tecnológica de la organización, por lo cual desde que el servidor y el servicio de sincronización sean implementados de forma correcta, se va a cumplir con los requisitos funcionales exigidos por los controles de la norma PCI DSS V 3.0.

4.6.1.4. Cuadro de relación de costos se implementación servidor de sincronización NTP con software comercial versus implementación servidor de sincronización NTP con software libre. Los costos derivados son de hardware y software (sistema operativo) debido a que el servicio de sincronización con un servidor NTP confiable es gratis, por lo cual se evaluaran los costos conforme a los diferentes sistemas operativos.

Cuadro 16. Relación Costos Implementación Servidor NTP

Descripción del costo	Sistema operativo		Comerciales
	Linux CentOS	Linux Red Hat	Windows Server
Licenciamiento Software	$0	$4'500.000	$4'000,000
Descripción del costo	**Sistema operativo**		**Comerciales**
	Linux CentOS	**Linux Red Hat**	**Linux CentOS**
Implementación	$2'000.000	$2'000.000	$2'000.000
Soporte	$0	Incluido en el valor del licenciamiento	Incluido en el valor del licenciamiento
Costos de Hardware	$2'000.002	$2'000.002	$2'000.002
TOTAL	$4'000.002	$8'500.002	$8'000.002

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 16 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento software

o Linux CentOS: dado que la aplicación es de libre distribución, no es necesario pagar un costo de licenciamiento por su uso.

o Linux Red Hat: Para la utilización de este sistema operativo no se debe pagar licenciamiento, el costo de referencia corresponde al valor de suscripción que se debe pagar para poder utilizar el Sistema Operativo.

o Windows Server: El costo de referencia corresponde a Windows Server 2012 R2 Data Center.

- Implementación:

o Linux CentOS: los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

o Linux Red Ha: Los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

o Windows Server: Los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

- Soporte:

o Linux Cantos: Por ser una herramienta libre no es necesario realizar pago de soporte, este es gratuito en la página del fabricante y es basado en correo electrónico y Foros de ayuda.

o Linux Red Ha: El derecho a soportes se incluye en el pago de suscripción, por lo cual no se requiere pagos adicionales, en el caso de este fabricante el soporte incluido es telefónico 7X24. sin embargo, también se puede realizar contratos de bolsas de horas presenciales para un soporte formal y personalizado con un valor adicional.

o Windows Server: El derecho a soportes se incluye dentro del mismo valor de licenciamiento, por lo cual no se requiere pagos adicionales, en el caso de este fabricante el soporte incluido es telefónico 7X24. sin embargo, también se puede realizar contratos de bolsas de horas presenciales para un soporte formal y personalizado con un valor adicional.

4.6.2 Conclusiones. La implementación de un servidor NTP se puede realizar en su totalidad con software libre, puede ser configurado en cualquier sistema operativo ya sea licenciado o libre, y de esta forma dar cumplimiento a los numerales exigidos por la norma PCI DSS V 3.0.

4.7 CIFRADO DE DATOS

El cifrado de datos, se puede entender como el proceso en el cual la información clara o legible se trasforma en ilegible, esto por medio algoritmos de cifrado compuesto por un conjunto de operaciones matemáticas que permiten transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible, esto también se le llama cifrado. La única forma de volver a hacer legible la información es introduciendo la clave del cifrado.

El cifrado de datos tiene como finalidad, evitar la fuga de información haciendo que la información no sea transmitida o almacenada en texto claro, lo que permite, que en caso de que se intercepte una comunicación o que se perdiere un dispositivo con información de una organización, esta no pueda ser usada de forma malintencionada o se pueda ver afectada la confidencialidad de la información.

La norma PCI-DSS, exige la implementación de herramientas de cifrado para proteger la información y los servicios no seguros, por lo cual la implementación de herramientas o mecanismos de cifrado se vuelven obligatorios para el

cumplimiento de la norma, con la implementación de herramientas de cifrado es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[86]:

- *Numeral PCI DSS 2.2.3* Implemente funciones de seguridad adicionales para los servicios, protocolos o ademaos requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSEC VPN, para proteger los servicios no seguros, como NetBIOS, archivos compartidos, Telnet, FTP, etc.

- *Numeral PCI DSS 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 otros tipos de acceso administrativo que no sea de consola.

- *Numeral PCI DSS 3.4.1* Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios.

- *Numeral PCI DSS 3.6.2* Distribución segura de claves de cifrado.

- *Numeral PCI DSS 3.6.3* Almacenamiento seguro de claves de cifrado.

- *Numeral PCI DSS 3.6.6* Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido.

Nota: Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.

- *Numeral PCI DSS 4.1* Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger los datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas, como, por ejemplo, las siguientes:

  - Solo se aceptan claves y certificados de confianza.

  - El protocolo implementado solo admite configuraciones o versiones seguras.

[86]PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 80

o La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza.

o Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes:

- La Internet
- Tecnologías inalámbricas, incluso 802.11 y Bluetooth
- Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código)
- Servicio de radio paquete general (GPRS)
- Comunicaciones satelitales

• *Numeral PCI DSS 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.).

4.7.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [87]Gartner dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, (ver figura 6); el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho(NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

[87] GARTNERT, INC. Op. Cit. p. 72

Figura 6. Gartner herramientas de cifrado publicado Septiembre de 2014

Fuente: GARTNER. Magic Quadrant for Web Application Firewalls. [En línea]. [consultado el 15 de Junio del 2015]- Disponible en <http://www.gartner.com/technology /reprints.do?id=1-26MDU0D&ct=141230&st=sb>

4.7.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar el cifrado de datos son las siguientes:

- McAfee(Complete Data Protection)[88]
- Aranda (Aranda 360 ENDPOINT SECURITY)[89]
- Check Point[90]
- Luks[91]
- AES Crypt[92]
- IPSEC

[88] MCAFEE.MCAFEE Complete Data Protection. [En línea], [consultado el 23 de diciembre de 2015]. Disponible en: http://www.mcafee.com /es/products/complete-data-protection.aspx#vt=vtab-CaracterC3ADsticasyventajas

89 ARANDA SOFTWARE. Aranda 360. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://arandasoft.com/aranda-360/

90 CHECK POINT. Endpoint Remote Access VPN. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.checkpoint.com /products/endpoint-remote-access-vpn-software-blade/>

91 THE GUARDIAN PROJECT. LUKS: Disk Encryption. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://guardianproject.info /code/luks/>

92 AESCRYPT. AES. Crypt Documentation. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.aescrypt.com/documentation/>

Se hace claridad que se referencian módulos específicos de las marcas analizadas, porque las soluciones privadas adicional al módulo de firewall poseen otras características, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0 o que no corresponden a los numerales de cifrado de datos.

4.7.1.2 Cuadro de comparación de herramientas de cifrado comerciales y herramientas de cifrado libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 17 y 18 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0.

En el cuadro 17 y 18 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar una herramienta de cifrado, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de una herramienta de cifrado:

- **Cifrado de servicios de red**

Cuadro 17**.** Comparación herramientas de cifrado comerciales y herramientas de cifrado libres frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales			Software libre
	CheckPoint	Aranda	SSL	IPSEC
Numeral PCI DSS 2.2.3 Implemente funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSEC VPN, para proteger los servicios no seguros, como NetBIOS, archivos compartidos, Telnet, FTP, etc.	√	√	√	√
Numeral PCI DSS 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 otros tipos de acceso administrativo que no sea de consola.	√	√	√	√

Cuadro 17. (Continuación)

Requisito especifico	Comerciales			Software libre
	CheckPoint	Aranda	SSL	IPSEC
Numeral PCI DSS 4.1 Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger los datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas			√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Cifrado en estaciones y servidores**

Cuadro 18. Comparación herramientas de cifrado comerciales y herramientas de cifrado libres frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre		
	McAfee	Aranda	Luks	AES Crypt	IPSEC
Numeral PCI DSS 3.4.1 Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios.	√	√	√	√	√
Numeral PCI DSS 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.).	√	√	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.7.1.3 Cuadro de relación de funcionalidades de herramientas de cifrado comerciales versus herramientas de cifrado libres. En los cuadros 19 y 20 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra.

En los cuadros 19 y 20 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger una herramienta de cifrado.

En la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

- **Cifrado en servicios de red**

Cuadro 19**.** Relación de funcionalidades de herramientas de cifrado comerciales versus herramientas de cifrado libres

Requisito especifico	Comerciales		Software libre
	Checkpoint	Aranda	IPSEC
VPN	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Cifrado en estaciones y servidores**

Cuadro 20**.** Relación de funcionalidades de herramientas de cifrado comerciales versus herramientas de cifrado libres

Requisito especifico	Comerciales		Software libre	
	McAfee	Aranda	Luks	AES Crypt
Cifrado de disco	√	√	√	-
Cifrado de archivos	√	√		√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.7.1.4 Cuadro de relación de costos de herramientas de cifrado comerciales versus herramientas de cifrado libres

Cuadro 21**.** Relación costos herramientas de cifrado comercial vs herramientas de cifrado libre

Descripción del costo	Comerciales			Libres
	McAfee	Checkpoint	Aranda	IPSEC
Licenciamiento Software	$1’600.000 (20 licencias)	$14’917.242	$4’500.000 (20 licencias)	
Implementación	$2’000.000	$2’000.000	$2’000.000	$2’000.000
Soporte	Incluido con la adquisición del licenciamiento	$8’531.698	$586.788	-
Costos de Hardware	$4’599.990	$4’599.990	$4’599.990	-
TOTAL	$8’199.990	$30’048.930	$8’500.002	$2’000.000

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 21 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento software

o MCAFEE: El costo de referencia corresponde a la solución Complete Data Protection, en el cuadro de costos se incluyen licenciamiento para 20 estaciones.

o CHECKPOINT: El costo de referencia corresponde a la solución EndpointRemote Access VPN.

o Aranda: El costo de referencia corresponde a la solución Aranda 360 ENDPOINT SECURITY en el cuadro de costos se incluyen licenciamiento para 20 estaciones.

o IPSEC: Dado a que la aplicación de libre, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o McAfee: Los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

o Checkpoint: Los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

o Aranda: Los costos de implementación corresponden a instalación, configuración del servidor y parametrización de los dispositivos de la infraestructura tecnológica (20 horas).

o IPSEC: Los costos de implementación corresponden a configuración de los dispositivos de red, servidores y terminales (20 horas).

- Soporte:

o McAfee: El derecho a soportes se incluye dentro del mismo valor de licenciamiento como un servicio postventa, por lo cual no se requiere pagos adicionales, en el caso de este fabricante el soporte incluido es telefónico 7X24, sin embargo, también se puede realizar contratos de bolsas de horas presenciales para un soporte más formal y personalizado por un valor adicional.

o Checkpoint: Se debe pagar contrato de soporte, Incluye soporte telefónico 7X24 y en caso de ser necesario soporte especializado presencial.

o Aranda: Soporte coste por licencia, el soporte es 7X24 telefónicamente.

o IPSEC: Es una herramienta que viene incluida en la mayoría de los dispositivos, no es factible establecer un costo de soporte, ya que esto puede corresponder a garantías o clausulas en la adquisición de los diferentes dispositivos.

- Costos de hardware

o McAfee: Es necesario la adquisición de un servidor que cumpla con las especificaciones de hardware y Software (Sistema Operativo) para la instalación de la consola de administración para la gestión centralizada de estaciones.

- Memoria UDIMM de 8 GB
- Disco duro cableado de 1 TB
- Procesador Intel® Xeon® E3-1220 v3, 3,1 GHz
- Sistema Operativo Windows Server® 2012 R2, FoundationEdition

o Checkpoint: Es necesario la adquisición de un servidor que cumpla con las especificaciones de hardware y Software (Sistema Operativo).

- Memoria UDIMM de 8 GB
- Disco duro cableado de 1 TB

- Procesador Intel® Xeon® E3-1220 v3, 3,1 GHz
- Sistema Operativo Windows Server® 2012 R2, FoundationEdition

o Aranda: Es necesario la adquisición de un servidor que cumpla con las especificaciones de hardware y Software (Sistema Operativo) para la instalación de la consola de administración para la gestión centralizada de estaciones.

- Memoria UDIMM de 8 GB
- Disco duro cableado de 1 TB
- Procesador Intel® Xeon® E3-1220 v3, 3,1 GHz
- Sistema Operativo Windows Server® 2012 R2, FoundationEdition

4.7.2 Conclusiones. La implementación de herramientas libres de cifrado para el cumplimiento de los numerales de la norma es factible en la gran mayoría de los puntos, sin embargo, una sola herramienta tanto en las herramientas libres como comerciales no contienes todas las funcionalidades para el cumplimiento de la totalidad de los numerales, por lo cual es necesario la implementación de varias herramientas para cubrirlos.

En el caso del numeral 2.3 de la norma, no es factible su cumplimiento con herramientas libres, ya que es necesario certificados SSL para aplicaciones web, estos certificados deben ser adquiridos o comprados a una entidad autorizada.

Los demás puntos pueden ser cubiertos con la implementación de las herramientas libres Luks, AES CryptyIPSEC VPN.

4.8 DLP COMERCIAL VERSUS DLP LIBRE

DLP es un software desarrollado para prevenir la perdida de datos, su sigla en inglés significa DLP (Data loss/leakprevention)[93], este tipo de soluciones están diseñadas para ayudar a las empresas a prevenir la perdida de información valiosa, para el caso práctico y refiriéndose a la norma PCI DSS V3.0 es necesario contar con una solución de DLP para evitar que los números de tarjeta habiente sean transmitidos fuera del entorno empresarial o fuera del entorno seguro de manera intencional o con fines delictivos.

SI bien la norma aconseja que no se presente el almacenamiento de números de tarjeta[94] ni ninguna de las pistas en claro, en ocasiones es necesario hacer uso de esta información por procesos propios de las empresas, para tal caso es necesario

[93] McAfee. Data Loss Prevention software. En línea], [citado el 15 de Junio del 2015]. Disponible en: http://www.mcafee.com/es/products/dlp-endpoint.aspx
[94] PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 83

contar con un software que ayude a las empresas a prevenir que esta información sea expuesta a personas no autorizadas.

Con la implementación de un software de DLP es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[95]:

- *Numeral PCI DSS4.2* 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.).

4.8.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia la herramienta privada líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [96]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, (ver figura 7);

El cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho (NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

[95] Ibíd., p. 92
[96]GARTNERT, INC. Op. Cit. p. 85

Figura 7. Cuadro de Gartner DLP publicado julio 2014

Fuente: GARTNER. Aware Data loss Prevention (DLP). [En línea], [consultado el 15 de Junio del 2015]- Disponible en: http://www.bytes.co.uk/info/technology-updates/gartner-recognizes-websense-market-leader-2014-dlp-magic-qua/>

4.8.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar software de DLP son las siguientes:

- McAfee DLP (Modulo de DLP)
- Symantec DLP (Modulo de DLP)
- Open DLP

Se hace claridad que se referencian módulos específicos de las marcas analizadas, porque las soluciones privadas adicional al módulo de software de DLP poseen otras características, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

4.8.1.2 Cuadro de comparación de DLP´S comerciales y DLP´S libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 22 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0.

En el cuadro 22 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un software de DLP, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un software de DLP:

Cuadro 22**.** Comparación software DLP comercial vs libres frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	**Comerciales**		**Software libre**
	McAfee DLP	**Symantec Data LossPrevention**	**OpenDLP**
Numeral PCI DSS 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.).	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.8.1.3 Cuadro de relación de funcionalidades de DLP´S comerciales versus DLP´S libres. En el cuadro 23 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 23 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características[97] que deben ser tomadas en cuenta al momento de escoger un DLP, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 23. Comparación software DLP comercial VS DLP libres

Atributos	Comerciales		Software libre
	McAfee DLP	**Symantec DLP**	**Open DLP**
Generación de reportes	PDF, XML, CSV	PDF, XML, CSV	PDF, XML, TXT
Actualizaciones automáticas	Desde casa matriz	Desde casa matriz	Manuales
Multiplataforma	Windows, Linux, AIX, OS	Windows, Linux, AIX, OS	Windows, Linux, AIX, OS
Requiere instancia de base de datos	Maneja una instancia independiente	La BD es embebida	No maneja
Consola centralizada	SI	SI	SI
Límite de direcciones IP	Ilimitado	Ilimitado	Una a la vez

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

[97] DEVICELOCK TECHNOLOGY. Prevent Devastating Data Leaks by Securing the Endpoints of Your Network. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.devicelock.com/products/>

*OPENDLP – FREE & OPEN-SOURCE. Pérdida libre y de código abierto de datos prevención de herramientas. [en línea]. [consultado el 15 de junio del 2015]. disponible en: http://www. darknet.org. uk/2010/05/opendlp-free-open-source-data-loss-prevention-dlp-tool/

*SYMANTEC. Symantec Data Loss Prevention. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.symantec.com/es/mx/data-loss-prevention/>

MCAFEE.MCAFEE DLP Endpoint.[Enlínea], [consultado el 15 de Junio del 2015]. Disponible en:.<http://www.mcafee.com/es/products/dlp-endpoint.aspx>

4.8.1.4 Cuadro de relación de costos de DLP´S comerciales versus DLP´S libres

Cuadro 24. Relación de costos software DLP comercial vs libres

Descripción del costo	Comerciales		Software libre
	McAfee DLP	Symantec DLP	Open DLP
Licenciamiento de la herramienta para 100 dispositivos	$25'970.000	$27'295.000	$0
Implementación	$8'000.000	$8'000.000	$5'000.000
Derechos de subscripción anual	$6'492.500	$6'823.750	$0
Soporte 50 horas anuales	$10'000.000	$10'000.000	$5'000.000
Costos de hardware	$11'236.000	$11'236.000	$11'236.000
Total	$61'698.500	$63'354.750	$21'236.000

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 24 de costos:(todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o MCAFEE DLP: El costo referenciado obedece a la suite total protection for data.

o SYMANTEC DLP: El costo referenciado obedece a la suite Symantec Data LossPrevention.

o OPEN DLP: Dado que OPEN DLP es desarrollado por el proyecto OPEN DLP FREE[98] la cual se acoge a la filosofía de software de libre distribución, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o MCAFEE DLP: Los costos de implementación planteados por McAfee son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo

[98]OPENDLP – FREE & OPEN-SOURCE. Op. cit. p. 95

McAfee, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.
o SYMANTEC DLP: Los costos de implementación planteados por Symantec son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo Symantec, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.

o OPEN DLP: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de DLP se requieren alrededor de 50 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o MCAFEE DLP: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o SYMANTEC DLP: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o OPEN DLP: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [99]donaciones.

- Soporte:

o MCAFEE DLP: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o SYMANTEC DLP Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o OPEN DLP: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000.

[99]FUNDACIÓN GNU. Op. Cit. p. 69

- Costos de hardware:

o MCAFEE DLP: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

o SYMANTEC DLP: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

o OPEN DLP: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

4.8.2 Conclusiones. Las soluciones de DLP privadas frente a la solución libre no presentan desventajas a nivel funcional, por este motivo es totalmente recomendable adquirir e instalar la aplicación OPEN DLP, ya que esto implica ahorros en costos de implementación y mantenimiento.

4.9 SOFTWARE DE DESCUBRIMIENTO DE DATOS DE TARJETA COMERCIAL VERSUS SOFTWARE DE DESCUBRIMIENTO DE DATOS DE TARJETA LIBRE

El[100] descubrimiento de datos de tarjetas en un ambiente empresarial en donde se busca adquirir una certificación en la norma PCI DSS V 3.0 es fundamental, ya que es la base para generar el inventario de activos que van a ser parte del alcance de la certificación.

Es necesario aclarar que no todos los activos tecnológicos de la empresa hacen parte del alcance al momento de ser revisados para una certificación PCI DSS V 3.0, únicamente se toman en cuenta los activos que procesen, almacenen o transmitan archivos con datos de tarjeta habientes, por eso contar con un software de descubrimiento de datos de tarjetas en vital para consolidar este insumo.

Con la implementación de un software de descubrimiento de datos de tarjeta es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[101]:

- *Numeral PCI DSS3.1* Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.

- *Numeral PCI DSS3.2* No almacene datos confidenciales de autenticación después de recibir la autorización.

- *Numeral PCI DSS3.2.1*No almacene contenido completo de ninguna pista de la banda magnética.

- *Numeral PCI DSS3.2.2* No almacene el valor ni el código de validación de tarjetas.

- *Numeral PCI DSS3.2.3*No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.

---

[100] CONTROLCASE. Software de Descubrimiento de Datos para Tarjetas de Crédito y Datos de los Tarjetahabientes para PCI DSS. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://www.controlcase.com/es/data_discovery.php

[101]PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 92

4.9.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia una de las herramientas privadas líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [102]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, (ver figura 8); el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho (NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

Figura 8. Gartner Software Descubrimiento de Tarjetas publicado Julio de 2014

Fuente Gartner. recognizes-websense-market-leader. [En línea], [consultado el 23 de noviembre de 2015]. Disponible en: http://www.bytes.co.uk/info/technology-updates/gartner-recognizes-websense-market-leader-2014-dlp-magic-qua/

[102]GARTNERT, INC. Op. Cit. p. 93

4.9.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar software de descubrimiento de datos de tarjetas son las siguientes:

- McAfee DLP (Modulo de DLP)
- Control Case (Modulo de DLP)
- CCSRCH

Se hace claridad que se referencian módulos específicos de las marcas analizadas, porque las soluciones privadas adicional al módulo de software de DLP poseen otras características, que, si bien pueden dar valor agregado a una compañía, son desestimadas al momento de referirse al estricto cumplimiento de la norma PCI DSS V 3.0.

En el caso de las herramientas privadas se hace referencia al módulo de DLP, porque este mismo modulo tiene la capacidad de realizar el escaneo sobre los activos para realizar el descubrimiento de los datos de tarjetas.

4.9.1.2 Cuadro de comparación de software de descubrimiento de datos de tarjeta comerciales y software de descubrimiento de datos de tarjeta libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 25 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0.

En el cuadro 25 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un software de descubrimiento de datos de tarjetas, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un software de descubrimiento de datos de tarjetas:

Cuadro 25**.** Comparación software de descubrimiento de tarjetas comercial vs libres frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Software libre
	McAfee DLP Discover	**Control Case Data Discovery**	**CCSRCH**
Numeral PCI DSS 3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.	√	√	√
Numeral PCI DSS 3.2 No almacene datos confidenciales de autenticación después de recibir la autorización.	√	√	√
Numeral PCI DSS 3.2.1 No almacene contenido completo de ninguna pista de la banda magnética.	√	√	√
Numeral PCI DSS 3.2.2 No almacene el valor ni el código de validación de tarjetas.	√	√	√
Numeral PCI DSS 3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.	√	√	√

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.9.1.3 Cuadro de relación de funcionalidades de software de descubrimiento de datos de tarjeta comerciales versus software de descubrimiento de datos de tarjeta libres. En el cuadro 26 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 26 se utilizan tres columnas principales.

La primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un software de descubrimiento de datos, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 26. Comparación software de descubrimiento de tarjetas comercial vs libres

Atributos	Comerciales		Software libre
	McAfee DLP Discover	Control Case Data Discovery	CCSRCH
Generación de reportes	PDF, XML, CSV	PDF, XML, CSV	TXT
Multi plataforma	Windows, Linux, AIX	Windows, Linux, AIX	Windows
Análisis programados	SI	SI	NO
Requiere instancia de base de datos	La BD es embebida	La BD es embebida	No maneja
Consola centralizada	SI	SI	NO
Límite de direcciones IP	Ilimitado	Ilimitado	Una a la vez

Fuente; Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.9.1.4 Cuadro de relación de costos de software de descubrimiento de datos de tarjeta comerciales versus software de descubrimiento de datos de tarjeta libres

Cuadro 27. Relación de costos software de descubrimiento de tarjetas comercial vs libres

Descripción del costo	Comerciales		Software libre
	McAfee DLP Discover	Control Case Data Discovery	CCSRCH
Licenciamiento de la herramienta para 100 dispositivos	$25’970.000	$27’295.000	$0
Implementación	$8’000.000	$6’000.000	$10’000.000
Derechos de suscripción anual	$6’492.500	$6’823.750	$0
Soporte 100 horas anuales	$10’000.000	$10’000.000	$10’000.000
Costos de hardware	$11’236.000	$0	$0
Total	$61’698.500	$50’118.750	$20’000.000

Fuente: Los Autores. Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 27 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o MCAFEE DLP Discover: El costo referenciado obedece a la suite total protection for data.

o Control Case Date Discovery: El costo referenciado obedece a la suite de soluciones para cumplimiento de la norma PCI DSS de Control Case

o CCSRCH: Dado que CCSRCH es desarrollado por el proyecto GNU [103] la cual se acoge a la filosofía de software de libre distribución, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o MCAFEE DLP Discover: Los costos de implementación planteados por McAfee son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo McAfee, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.

o Control Case Date Discovery: Los costos de implementación planteados por Control Case son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo Control Case, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.

o CCSRCH: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de software de descubrimiento de datos de tarjetas se requieren alrededor de 100 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o MCAFEE DLP Discover: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

[103] CAUDILL. CCSRCH - Open Source PAN / Credit Card Scanner. [En línea]. [citado el 15 de Junio del 2015]. Disponible en: http://adamcaudill.com/ccsrch/>

o Control Case Date Discovery: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o CCSRCH: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [104]donaciones.

- Soporte:

o MCAFEE DLP Discover: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o Control Case Date Discovery Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o CSRCH: Se calculó una bolsa de 100 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000. la cantidad de horas es superior a comparación de las soluciones privadas, ya que esta solución es necesario ejecutarla maquina por maquina al no contar con una consola centralizada, lo cual es más dispendioso y toma más tiempo.

- Costos de hardware:

o MCAFEE DLP Discover: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

[104] FUNDACIÓN GNU. Op. Cit. p. 97

o Control Case Date Discovery: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o CCSRCH: Esta herramienta se instala directamente sobre el equipo al cual se le va a realizar el descubrimiento, y se debe realizar maquina por máquina, por este motivo es necesario adquirir hardware adicional.

4.9.2 Conclusiones. La implementación de un software de descubrimiento de datos de tarjetas libre es mucho más económica que la de soluciones privadas, se puede hablar de un ahorro del 65% en promedio, es necesario tener en cuenta que la herramienta de software libre genera mucha más administración, ya que, al no contar con una consola centralizada, se hace necesario realizar el despliegue del producto y la ejecución del descubrimiento activo por activo.

4.10 SOFTWARE DE MONITOREO DE INTEGRIDAD DE ARCHIVOS COMERCIAL VERSUS SOFTWARE DE MONITOREO DE INTEGRIDAD DE ARCHIVOS LIBRE

El software de monitoreo de integridad de archivos[105] se encarga como su nombre lo indica de monitorear archivos base del sistema con el fin de garantizar que estos no sean alterados ya sea por los usuarios o por software malicioso, adicionalmente a los archivos base del sistema, tienen la capacidad de monitorear rutas especificas a fin de prevenir la alteración o acceso a archivos que el usuario o la empresa defina como críticos.

Para el caso de la certificación PCI DSS V 3.0 esta exige que se monitoree todo acceso a archivos que contengan datos de tarjetas, es necesario garantizar la integridad de dicha información ya que su alteración o manipulación puede ser realizada con fines fraudulentos, por tal motivo es imperativo realizar monitoreo sobre esta información utilizando un software de monitoreo de integridad de archivos.

Con la implementación de un software de monitoreo de integridad de archivos es posible dar cumplimiento a los siguientes numerales de la norma PCI DSS V 3.0[106]:

- *Numeral PCI DSS10.5.5* Utilice el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen.

[105] MCAFEE.SECURITY Management. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.mcafee.com/us/products/security-management/index.aspx>
[106] PCI SECURITY STANDARDS COUNCIL. Op. Cit. p. 99

- *Numeral PCI DSS11.5*Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de monitorización de integridad de archivos).

- *Numeral PCI DSS12.10.5*Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

4.10.1 Comparación de herramientas libres contra herramientas privadas. Para realizar la comparación se toma como referencia una de las herramientas privadas líder del mercado y otra herramienta privada de gama media contra la herramienta de software libre mejor referenciada, para las herramientas privadas se tomará la calificación dada por la empresa estadounidense [107]Gartnert dedicada a la consultoría y la investigación de tecnologías informáticas, esta empresa utiliza una metodología conocida como el cuadrante mágico, ver figura 9; el cuadrante mágico básicamente es un plano cartesiano en donde ellos ubican a las marcas evaluadas, las ubicaciones o resultados son líderes (LEADERS), visionarios (VISIONARIES), retadores (CHALLENGERS) y jugadores de nicho(NICHE PLAYERS), para el caso de las herramientas libres Gartner no las evalúa ni califica, ya que para ser evaluado por Gartner es necesario estar subscrito y adicionalmente Gartner hace parte de la maquinaria privada, por ende va totalmente en contra de la filosofía del software libre.

Figura 9. Gartner software de monitoreo de integridad de archivos publicado junio de 2014.

Fuente GARTNER. Secutity informtion and event management. [en línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://blogs.mcafee.com/business/security-connected/mcafee-leader-in-gartner-magic-quadrant-siem>

[107]GARTNERT, INC. Op. Cit. p. 100

4.10.1.1 Herramientas evaluadas. Las herramientas que se van a tener en cuenta para evaluar Firewall son las siguientes:

- McAfee change control
- Trustwave
- OSSEC

4.10.1.2 Cuadro de comparación de software de monitoreo de integridad de archivos comerciales y software de monitoreo de integridad de archivos libres frente al cumplimiento de la norma PCI DSS V 3.0. En el cuadro 28 que se presenta a continuación se hace referencia al cumplimiento que puede o no brindar cada una de las herramientas elegidas frente a los numerales de la norma PCI DSS V 3.0, en el cuadro 28 se utilizan tres columnas principales la primera (requisito especifico) hace referencia al numeral de la norma que para su cumplimiento requiere implementar un software de monitoreo de integridad de archivos, en la columna dos (comerciales), se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cumple con el requisito se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, es necesario acotar que solo se tienen en cuenta numerales que para su cumplimiento requieren de la implementación de un software de monitoreo de integridad de archivos.

Cuadro 28**.** Comparación software de monitoreo de integridad de archivos comercial vs libres frente al cumplimiento de la norma PCI DSS V 3.0

Requisito especifico	Comerciales		Softwar e libre
	McAfeechan ge control	Radware	OSSEC
Numeral PCI DSS 10.5.5 Utilice el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas.	√	√	√
Numeral PCI DSS 11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de monitorización de integridad de archivos) para alertar al personal sobre modificaciones no autorizadas de archivos críticos del sistema.	√	√	√
Numeral PCI DSS 12.10.5 Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.	√	√	√

Fuente: Los Autores. Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.10.1.3. Cuadro de relación de funcionalidades de software de monitoreo de integridad de archivos comerciales versus software de monitoreo de integridad de archivos libres. En el cuadro 29 se relacionan funcionalidades técnicas de las herramientas necesarias para realizar su administración de una forma más práctica y sencilla, las funcionalidades son juzgadas netamente por su existencia o usencia, mas no se entra a definir si una es superior o inferior a la otra, en el cuadro 29 se utilizan tres columnas principales la primera (funcionalidad) hace referencia a esas características que deben ser tomadas en cuenta al momento de escoger un software de monitoreo de integridad de archivos, en la columna dos (Comerciales) se hace referencia a las marcas comerciales analizadas y la columna tres (Software libre) hace referencia a la o las herramientas de software libre analizadas, si la herramienta cuenta con la funcionalidad se coloca un visto bueno, de lo contrario la casilla se encuentra vacía, el objetivo de este análisis es plasmar si las herramientas analizadas están en capacidad de dar cumplimiento frente a una revisión de la norma PCI DSS V 3.0.

Cuadro 29. Comparación software de monitoreo de integridad de archivos comercial vs libres

Atributos	**Comerciales**		**Software libre**
	McAfee change control	**Trustwave**	**OSSEC**
Generación de reportes	PDF, XML, CSV	PDF, XML, CSV	XML, TXT
Alertas en tiempo real	SI	SI	SI
Multiplataforma	Windows, Linux, AIX	Windows, Linux, AIX	Windows, Linux, AIX
Consola centralizada	SI	SI	SI
Límite de activos monitoreados	Ilimitado	Ilimitado	Ilimitado

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

4.10.1.4 Cuadro de relación de costos de software de monitoreo de integridad de archivos comerciales versus software de monitoreo de integridad de archivos libres.

Cuadro 30. Relación de costos software de monitoreo de integridad de archivos comercial vs libres

Descripción del costo	Comerciales		Software libre
	McAfee change control	Trustwave	OSSEC
Licenciamiento de la herramienta para 100 dispositivos	$23'850.000	$16'430.000	$0
Implementación	$8'000.000	$6'000.000	$5'000.000
Derechos de suscripción anual	$5'962.500	$4'107.500	$0
Soporte 50 horas anuales	$10'000.000	$10'000.000	$5'000.000
Costos de hardware	$11'236.000	$11'236.000	$11'236.000
Total	$59'048.500	$47'773.500	$21'236.000

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

A continuación, se explica el cuadro 30 de costos: (todos los costos están expresados en pesos Colombianos COP)

- Licenciamiento de la herramienta:

o MCAFEE CHANGE CONTROL: se toman como base 100 activos para el licenciamiento de esta herramienta.

o TRUSTWAVE: se toman como base 100 activos para el licenciamiento de esta herramienta.

o OSSEC: Dado que OSSEC es desarrollado por el proyecto[108] OSSEC el cual se acoge a la filosofía de software de libre distribución, no es necesario pagar un costo de licenciamiento por su uso.

- Implementación:

o MCAFEE CHANGE CONTROL: Los costos de implementación planteados por McAfee son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el

[108] OSSEC. PCI Solution. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.ossec.net/files/ossec-PCI-Sol33ution-2.0.pdf>

mismo Check Point, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.

o TRUSTWAVE: Los costos de implementación planteados por Trustwave son relativamente elevados, debido al nicho de mercado que manejan y a que los ingenieros que implementan deben ser mano de obra certificada por el mismo Check Point, esto genera que los costos sean más elevados, en promedio la hora de un ingeniero certificado esta alrededor de los $200.000.

o OSSEC: En promedio la hora de mano experta en plataformas de software libre esta alrededor de los $100.000 y para implementar una solución de tipo firewall se requieren alrededor de 50 horas, ahora bien, si la empresa cuenta con un recurso calificado en software libre, puede existir una disminución adicional en los costos.

- Derechos de subscripción anual:

o MCAFEE CHANGE CONTROL: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.

o TRUSTWAVE: se debe pagar un derecho de suscripción anual el cual le da derecho al comprador a recibir actualizaciones de software y parches de seguridad, normalmente equivale a un rango entre un 20% y un 25% del costo de adquisición.
o OSSEC: No es necesario pagar derechos de suscripción anual, las actualizaciones están disponible en la página del fabricante. Si bien no se cobran derechos por actualizaciones si existe la posibilidad de realizar [109]donaciones.

- Soporte:

o MCAFEE CHANGE CONTROL: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o TRUSTWAVE: CHECK POINT: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 200.000.

o OSSEC: CHECK POINT: Se calculó una bolsa de 50 horas anuales para atender requerimientos e inquietudes que puedan presentarse, el promedio del costo por hora de mano de obra certificada es del orden de $ 100.000.

[109] FUNDACIÓN GNU. Op. Cit. p. 105

- Costos de hardware:

o MCAFEE CHANGE CONTROL: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

o TRUSTWAVE: Por tratarse de un appliance no es necesario realizar inversiones en hardware adicional.

o OSSEC: Es necesario adquirir un servidor que provee características adecuadas para el desempeño del software, si bien el fabricante hace referencia únicamente a las características mínimas de maquina exigidas, es importante no sub dimensionar las mimas, a fin de proveer al software los recursos para un óptimo funcionamiento. Por eso se plantea la posibilidad de contar con un servidor de las siguientes características técnicas:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

4.10.2 Conclusiones. Tanto las herramientas de monitoreo de integridad de archivos privadas, como la herramienta libre dan cubrimiento a las exigencias de la norma PCI DSS V 3.0 por lo tanto y tomando en cuenta la gran diferencia en costos es aconsejable optar por la herramienta OSSEC.

5. GUÍA DE IMPLEMENTACIÓN DE HERRAMIENTAS TECNOLÓGICAS DIRIGIDA A LAS PYMES PARA DAR CUMPLIMIENTO A LA NORMA INTERNACIONAL PCI DSS V3.0

Esta guía fue concebida para ayudar a las pequeñas y medianas empresas que procesen, transmitan o almacenen datos de tarjeta habientes y que quieran o deban buscar la certificación PCI DSS V 3.0, el propósito es ayudar a estas empresas a cumplir con los requisitos del estándar que involucren un componente tecnológico de tipo software, y está dirigida en especial a personal responsable de mantener la seguridad informática y de la información en estas empresas, para llevar a cabo su aplicación es necesario tener conocimientos técnicos en implementación e implantación de proyectos de software libre y sistemas operativos LINUX en todas sus versiones, es posible que las empresas no cuenten con un recurso que cumpla con los niveles de conocimiento exigidos, por lo tanto debe contemplar la posibilidad de una contratación directa o una tercerización del servicio.

Para poder cumplir con los requisitos de la norma PCI DSS V 3.0 que involucran la instalación, configuración y administración de un componente tecnológico de tipo software esta guía recomienda la utilización de software de naturaleza libre, es decir que no es necesario pagar costos de licenciamiento por su utilización. El hecho de no tener que pagar por la utilización del software impacta positivamente los costos de ejecución de un proyecto de certificación en la norma PCI DSS V 3.0, esto a su vez redunda en poder llevar a niveles superiores la competitividad y presencia en el mercado de la compañía que decida o deba certificarse en la norma.

NOTA: Esta guía es un documento técnico que proporciona orientación de que herramientas de software libre que pueden cumplir con las solicitudes realizadas en la norma PCI DSS V 3.0 en los *numerales 1.1.4, 1.2, 1.2.1, 1.2.3, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 2.2.3, 2.3, 3.4.1, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3, 3.5, 3.6.2, 3.6.3, 3.6.6, 4.1, 4.2, 5.1, 5.1.1, 5.2, 5.3, 6.6, 7.2, 7.2.1, 7.2.2, 7.2.3, 10.4, 10.4.1, 10.4.3, 10.5.5, 11.1, 11.2, 11.2.1, 11.3.3, 11.4, 11.5, 12.10.5.* se basa en los resultados de la investigación contenida en el proyecto de grado ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE FIREWALL DE RED, IPS, NTP, FILTRADO DE CONTENIDO, DLP, DESCUBRIMIENTO DE DATOS DE TARJETA, FIREWALL DE APLICACIÓN, MONITOREO DE INTEGRIDAD DE ARCHIVOS, ESCÁNER DE VULNERABILIDADES, ANTIVIRUS Y CIFRADO DE DATOS, PARA EL CUMPLIMIENTO DE LOS CONTROLES DE LA NORMA DE SEGURIDAD DE DATOS PCI DSS V3.0 QUE EXPLÍCITAMENTE IMPLICAN ADQUIRIR E IMPLEMENTAR HERRAMIENTAS TECNOLÓGICAS DE SEGURIDAD INFORMÁTICA PARA SU CUMPLIMIENTO del programa de especialización en seguridad informática de la Universidad Piloto de Colombia corte 22, elaborada por Javier Perdomo, Hugo Casallas y Julio Vargas en el mes de Junio de 2015.

La guía en si no ofrece información completa acerca de la forma de cumplir con el 100% de la norma PCI DSS V 3.0, únicamente relaciona los numerales anteriormente mencionados y no se convierte en un asesoramiento legal, solo presenta información técnica y objetiva acerca del cumplimiento exigido, se recomienda no consultar únicamente esta guía para obtener asesoramiento acerca de la forma de tratar los requisitos normativos.

5.1 HERRAMIENTAS EVALUADAS FRENTE AL CUMPLIMIENTO DE LOS REQUISITOS

A continuación, se exponen cada una de las herramientas evaluadas y los puntos de la norma que se pueden cumplir con cada una de ellas:

- Firewall de Red (Numerales PCI DSS,1.1.4 – 1.2 – 1.2.1 – 1.2.3 – 1.3 – 1.3.1 – 1.3.2 – 1.3.3 – 1.3.4 – 1.3.5 – 1.3.6 – 1.3.7 – 1.3.8 – 7.2 – 7.2.1 – 7.2.2 – 7.2.3 – 12.10.5)

- IPS (Numerales PCI DSS, 11.1 – 11.4)

- NTP (Numerales PCI DSS, 10.4 – 10.4.1 – 10.4.3)

- Filtrado de contenido (Numerales PCI DSS, 1.3 – 1.3.3 – 1.3.8)

- DLP (Numeral PCI DSS,4.2)

- Descubrimiento de datos de tarjeta (Numerales PCI DSS, 3.1 – 3.2 -3.2.1 – 3.2.2 – 3.2.3)

- Firewall de aplicación (Numerales PCI DSS, 6.6 – 12.10.5)

- Monitoreo de integridad de archivos (Numerales PCI DSS, 10.5.5 -11.5 – 12.10.5)

- Escáner de vulnerabilidades (Numerales PCI DSS, 11.2 -11.2.1 – 11.3.3)

- Antivirus (Numerales PCI DSS, 5.1 – 5.1.1 – 5.2 – 5.3)

- Cifrado de datos (Numerales PCI DSS, 2.2.3 – 2.3 – 3.4.1 – 3.6.2 – 3.6.3 – 3.6.6 – 4.1 – 4.2)

5.2 RECOMENDACIONES GENERALES

ALCANCE PCI: Se define alcance PCI a todo activo que su función deba procesar, almacenar o transmitir datos de titular de tarjeta, estos activos serán el foco de la revisión en caso de querer buscar una certificación PCI DSS, para lograr la definición de este alcance es necesario contar con los siguientes insumos:

- Inventario de activos, se debe detallar la dirección IP del activo, el nombre, su función y quien lo administra.

- Identificar las razones de negocio que requieren que el activo procese, almacene o transmita datos de titular de tarjeta.

SOFTWARE BASE: Ya que esta guía promueve la utilización de software libre para lograr una reducción considerable en los costos tecnológicos generados al buscar una certificación en la norma PCI DSS V 3.0 La recomendación es implementar las herramientas recomendadas sobre LINUX en sus distribuciones CENTOS o DEBIAN, estos softwares son de libre distribución, es posible descargarlos de los siguientes sitios:

- CENTOS: http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1503-01.iso

- DEBIAN: https://www.debian.org/distrib/netinst

Asegúrese de descargar la versión más actualizada que encuentre disponible. Si tiene dudas acerca de la instalación del software base propuesto puede consultar la siguiente documentación:

- http://www.tecmint.com/centos-7-installation/

- https://debian-handbook.info/browse/stable/sect.installation-steps.html

NOTA: Posterior a la instalación del software base y el software de aplicación, es recomendable endurecer las características de seguridad del sistema, a continuación, encontrara información referente al caso en las siguientes fuentes:

- https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

Tener en cuenta que la documentación de endurecimiento de sistema de la distribución RED HAT de LINUX aplica para CENTOS, no se recomendó la versión RED HAT en un principio, ya que para mantenerla actualizada es necesario pagar un derecho de suscripción anual y esto se sale del esquema del software libre.

HARDWARE: Para que la aplicación le brinde un buen rendimiento tenga en cuenta las siguientes recomendaciones a la hora de elegir el hardware sobre el cual la va a instalar:

- https://www.centos.org/docs/5/html/Installation_Guide-en-US/ch-ent-table.html

- https://www.debian.org/releases/wheezy/i386/ch02s01.html.es

Las recomendaciones dadas por los fabricantes generalmente hacen referencia a los requerimientos mínimos de hardware para obtener un buen rendimiento, pero teniendo en cuenta que la guía está enfocada a pequeñas y medianas empresas que transmitan, almacenen o procesen datos de tarjetas, las cuales probablemente cuenten con una operación 7x24x365 es decir que nunca paran, la recomendación es implementar un hardware más robusto que no tenga problemas a la hora de una mayor exigencia, una propuesta es implementar la solución sobre el siguiente hardware:

- Procesador 3.0 GHZ Octa Core
- Memoria RAM 16 GB
- Arreglo de discos
- Espacio efectivo en discos 1 Tb
- Fuente de poder redundante
- 4 tarjetas de red

NOTA: Para el caso del arreglo de discos se recomienda utilizar RAID 1, para mayor profundización acerca de este tema puede consultar la siguiente documentación:

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux /6/pdf/Logical_Volume_Manager_Administration/Red_Hat_Enterprise_Linux-6-Logical_Volume_Manager_Administration-en-US.pdf

- https://debian-handbook.info/browse/stable/advanced-administration.html

Tener en cuenta que la documentación de la distribución RED HAT de LINUX aplica para CENTOS, no se recomendó la versión RED HAT en un principio, ya que para mantenerla actualizada es necesario pagar un derecho de suscripción anual y esto se sale del esquema del software libre.

5.3 HERRAMIENTAS DE SOFTWARE LIBRE ELEGIDAS PARA DAR CUMPLIMIENTO A LOS REQUISITOS EXIGIDOS POR LA NORMA PCI DSS V 3.0

A continuación, en el cuadro 31 se relaciona el software libre recomendado para cada una de las herramientas requeridas por los controles tecnológicos que exige la norma PCI DSS V 3.0

Cuadro 31**.** Herramientas de software libre seleccionadas para la implementación de la norma PCI DSS 3.0

Solución tecnológica exigida por la norma PCI DSS V 3.0	Solución de software libre propuesta
Firewall de red	IPtables
IPS	Snort
NTP	Basado en Linux
Filtrado de contenido	Squid
DLP	Open dlp
Descubrimiento de datos de tarjeta	Ccsrch
Solución tecnológica exigida por la norma PCI DSS V 3.0	**Solución de software libre propuesta**
Firewall de aplicación (WAF)	Modsecurity
Monitoreo de integridad de archivos	Ossec
Escáner de vulnerabilidades	*Open Vas
Antivirus	No aplica
Cifrado de datos	Luks – AESCrypt – IPsecVPN

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

5.4. EL QUE Y EL COMO DEL CUMPLIMIENTO DE CADA HERRAMIENTA FRENTE A LOS REQUISITOS DE LA NORMA PCI DSS V 3.0.

A continuación, se expone puntualmente cada herramienta frente al cumplimiento de la norma PCI DSS V 3.0, y se darán recomendaciones para su implementación, para recomendaciones técnicas acerca de software base por favor diríjase al numeral 5.2 de esta guía.

5.4.1 Firewall. Para esta herramienta se escogió el software IPTABLES, a continuación, se relacionan los sitios en los cuales se puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la 1.4.21, (fecha de revisión, 5 de octubre de 2015).
http://www.netfilter.org/projects/iptaq bles/files/iptables-1.4.21.tar.bz2

- Instalación y configuración de IPTABLES.

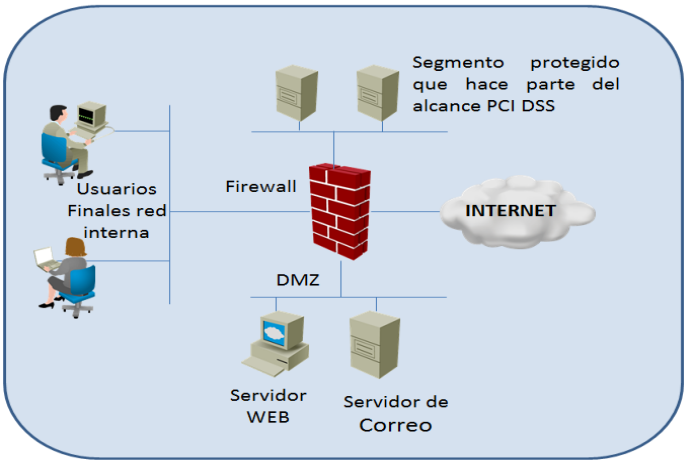
http://www.alcancelibre.org/staticpages/index.php/introduccion-iptables
http://www.linuxfromscratch.org/blfs/view/svn/postlfs/firewall.html

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 1.1.4** Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.

Recomendación: como puede observarse en la figura 10, es necesario un firewall en cada una de las conexiones hacia internet y entre cualquier DMZ y la red interna, es decir que todos los equipos que hacen parte del alcance PCI DSS deben estar segmentados en VLANS especiales y protegidos por un Firewall, con el fin de separar los segmentos de red de usuarios finales y servidores que no hacen parte del alcance PCI DSS, servidores que sean expuestos hacia internet que hagan parte del alcance deben estar ubicados en una red DMZ, a fin de separar estos servicios de la red interna y así obtener un mayor nivel de seguridad. Los segmentos de red que no hacen parte del alcance, deben estar separados de los segmentos de red que hacen parte del alcance. En un ambiente empresarial normalmente encontramos servidores dedicados a bases de datos, aplicaciones, servidores web y servicios internos o propietarios de la compañía, es de vital importancia identificar cuáles de estos activos transmiten, procesan o almacenan datos de tarjeta habientes y mediante la utilización de un firewall se deben separar lógicamente de los activos que no cumplan con esta condición, es decir activos que no procesan, transfieren o almacenan datos de tarjetas.

Figura 10. Topología acorde a requisito 1.1.4 de la norma PCI DSS.



Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Numeral PCI DSS 1.2** Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas.

Recomendación: Para dar cumplimiento a este punto es necesario definir reglas en el firewall que no permitan el acceso a personal no autorizado a activos que hagan parte del alcance PCI, todo lo que no haga parte de este alcance se considera como no confiable. Una buena práctica es dividir el entorno en segmentos de red de propósito específico tales como red interna, internet, proveedores, red Wireless, servidores WEB, servidores de aplicación y servidores de bases de datos, ver figura 10 Topología acorde a requisito 1.1.4 de la norma PCI DSS.

- **Numeral PCI DSS 1.2.1 Restrinja** el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.

Recomendación: Una vez establecidos los segmentos de red que hacen parte del ambiente de protección de datos de tarjeta, se deben establecer reglas de acceso en donde se especifiquen:

- La dirección IP que identifica el origen de la conexión.
- La dirección IP que identifica el destino de la conexión.
- Los servicios, puerto y protocolos que serán usados en la conexión.
- Acción a tomar, permitir o negar el acceso.

Estas configuraciones deben realizarse a fin de no permitir ningún servicio, puerto o protocolo innecesario, ya que los servicios que se encuentren configurados y no son usados pueden prestarse para permitir accesos no autorizados, la configuración en firewall debe estar en capacidad de negar el tráfico que no haya sido explícitamente autorizado, lo anterior se consigue con una regla de negación configurada como la última regla en firewall de la siguiente forma:

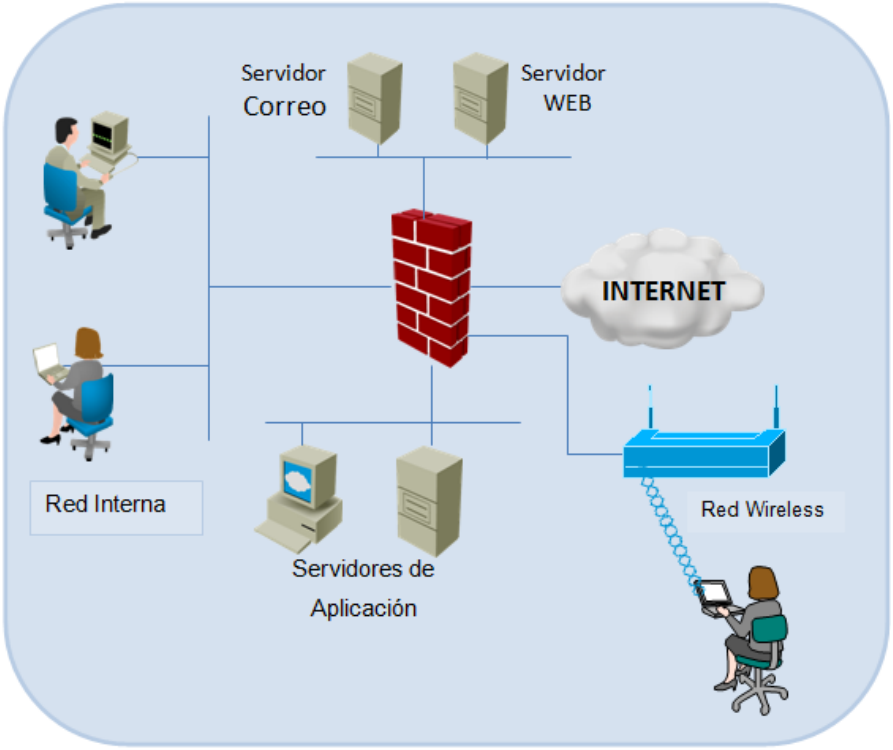
- IP origen any
- IP destino any
- Servicio, puerto o protocolo any
- Acción deny

- **Numeral PCI DSS 1.2.3** Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta.

Recomendación: Dado que la seguridad de las redes inalámbricas representa un punto de fácil penetración para una red, la norma exige mitigar este tipo de ataques realizando segmentación y aislamiento para estas redes, para dar

cumplimiento a la anterior exigencia es necesario segmentar la red inalámbrica en una red exclusiva que esté ubicada en un segmento de red distinta al segmento de ambiente protegido PCI DSS y que se encuentre limitada a través de firewall, es decir bajo ninguna circunstancia se debe tener redes inalámbricas directamente conectadas a la red interna o redes que hagan parte del alcance PCI DSS, ver figura 11.

Figura 11. Protección de red Wireless.



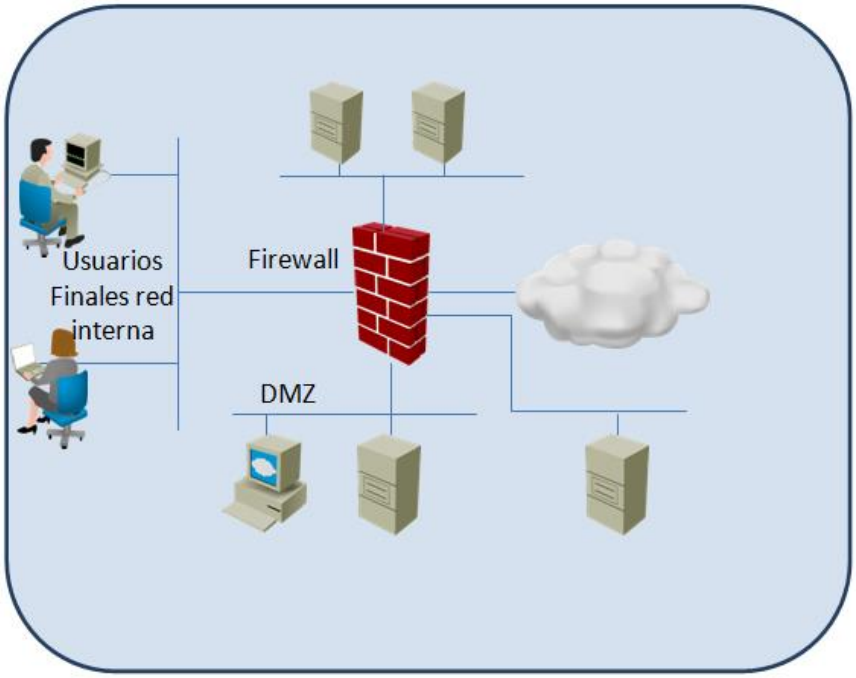
Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

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

Recomendación: Es necesario que las aplicaciones que prestan servicios que son expuestos en internet se encuentren ubicados sobre un segmento de red en una zona desmilitarizada o DMZ y protegidas a través de firewall, adicionalmente se debe hacer uso de la funcionalidad NAT (Network AddressTranslation) con el fin de no difundir la dirección IP real del servidor donde se aloja la aplicación expuesta. No se deben exponer direcciones IP del segmento que hace parte del alcance directamente sobre internet, ya que esta exposición de direccionamiento

IP real configurado sobre los servidores representa la posibilidad de que un atacante ingrese directamente al servicio y por ende al entorno protegido.

Figura 12**.** DMZ protegida por firewall



Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Numeral PCI DSS 1.3.1** Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.

Recomendación: Dada la naturaleza de una red DMZ la cual es exponer servicios a internet la hace especialmente vulnerable a ataques provenientes de internet, es necesario configurar el set de reglas de firewall de tal forma que estos servicios expuestos sean exclusivamente los necesarios, es decir para un servidor WEB como el que se observa en la figura 12 una regla de acceso en firewall debe configurarse como:

- IP origen Any

- IP destino La IP pública correspondiente al servidor WEB expuesto, esta IP no debe ser la IP real configurada sobre el servidor, esta IP corresponde a una IP de NAT la cual será dirigida al servidor WEB una vez la petición de conexión válida llegue al firewall.

- Servicio, dado que se trata de un servidor WEB se deben habilitar puertos correspondientes a estos servicios tales como puerto TCP 80 para protocolo HTTP y puerto TCP 443 correspondiente a protocolo HTTPS.

- Acción permitir.

Con la configuración anteriormente descrita se da cumplimiento a lo exigido por este punto de la norma PCI DSS.

- **Numeral PCI DSS 1.3.2** Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.

Recomendación: Todas las conexiones que son originadas desde internet deben llegar a una red DMZ, la configuración en firewall debe estar dispuesta de tal forma que las conexiones provenientes de internet no lleguen a la red interna o red que haga parte del alcance PCI DSS, ver figura 12, en este caso las dos redes que pueden recibir conexiones directamente desde internet son la DMZ no PCI DSS y la DMZ que hace parte del alcance PCI DSS.

- **Numeral PCI DSS 1.3.3** No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.

Recomendación: Todas las conexiones entrantes deben cumplir lo exigido en el numeral 1.3.2 de la norma PCI DSS versión 3.0, para el caso de las conexiones salientes hacia internet en todo caso debe disponerse de un firewall que proteja la salida de estas conexiones, lo anterior debido a que un computador o servidor infectado por un troyano puede iniciar conexiones hacia internet y puede ser una puerta trasera poniendo en riesgo la seguridad de la red.

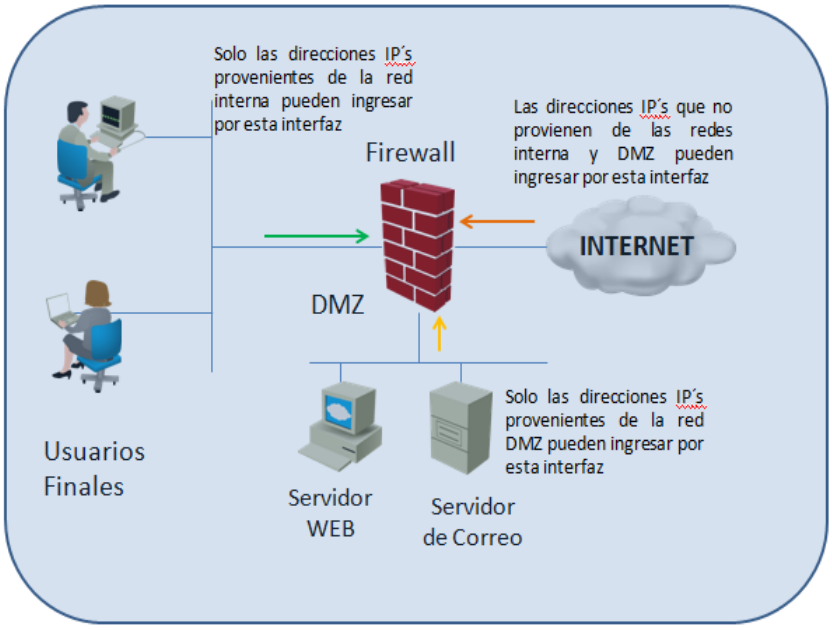
- **Numeral PCI DSS 1.3.4** Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.

Recomendación: Con el fin de evitar suplantaciones en direccionamiento IP de la red interna, se deben configurar filtros sobre cada una de las interfaces del firewall de tal forma que se legitime el origen de las conexiones y si estas provienen del segmento de red apropiado, es decir si existe una petición proveniente de internet con direccionamiento de una red interna aunque exista una regla en firewall que permita este acceso, el firewall debe estar configurado para negar la petición de conexión al validar que esta solicitud proviene de un segmento de red el cual no es el legítimo, este comportamiento puede ser observado en la gráfica 13 protección de suplantación.

Para un mayor detalle de cómo llevar a cabo el filtro de prevención de suplantación de direccionamiento IP “anti spoofing” puede dirigirse a la URL.

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf, Página 116 sección 2.8.6.“Malicious Software and Spoofed IP Addresses”.

Figura 13. Protección de suplantación.



Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Numeral PCI DSS 1.3.5** No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.

Recomendación: Las solicitudes de conexión provenientes de los servidores que hacen parte del ambiente de datos de tarjeta y cuyo destino es internet, deben estar plenamente identificados y se debe garantizar que estas conexiones son autorizadas y se deben limitar a las explícitamente necesarias, lo anterior con el fin de no dejar posibles puertas traseras que pongan en riesgo la seguridad de la red.

- **Numeral PCI DSS 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”).

Recomendación: La inspección completa de paquetes “state full inspection”, consiste en hacer validación del estado de las conexiones TCP en su saludo de tres vías en donde la conexión se establece al intercambiar tres paquetes así:

- Paquete 1, el host A requiere establecer una conexión con el host B, para ello envía un paquete con la bandera SYNC en 1.

- Paquete 2, el host B acepta la conexión y responde con las banderas SYNC y ACK en 1.

- Paquete 3, el host A confirma la recepción del paquete enviando la bandera ACK en 1.

- Cuando se da el envío y recepción de estos tres paquetes entre los hosts A y B la conexión está lista para ser usada e intercambiar paquetes y flujo de datos.

Sólo cuando se da el saludo de tres vías debe haber flujo de datos entre dos equipos, el firewall debe estar configurado de tal forma que valide su tabla de conexiones y al recibir una petición de conexión de tipo ACK o PUSH, FIN, RESET, sin haberse establecido el saludo de tres vías esta debe ser negada ya que pertenece a una solicitud no válida.

Para un mayor detalle y como realizar la configuración de inspección completa de paquetes o state full inspection diríjase a la URL.

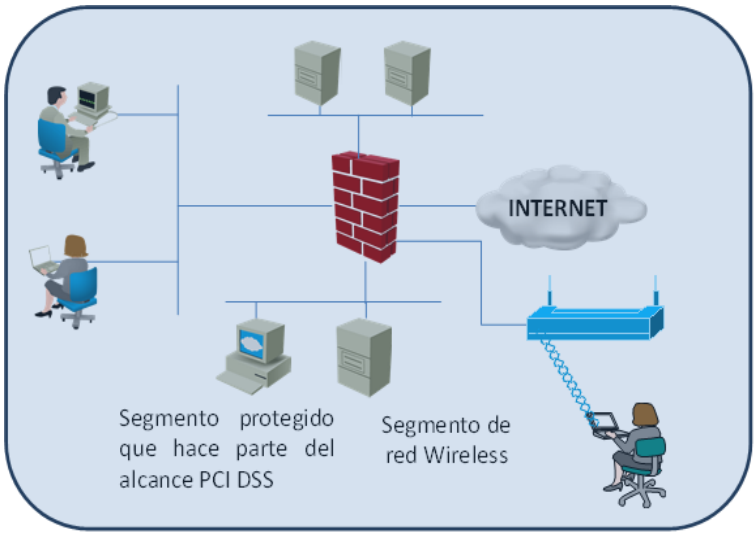
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

Página 117 sección 2.8.7.“IPTables and Connection Tracking”.

- **Numeral PCI DSS 1.3.7** Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.

Recomendación: Se debe crear un segmento de red específico para bases de datos que hacen parte del entorno de datos de tarjeta a fin de aislar y proteger la información sensible allí contenida; la norma exige prevenir accesos provenientes tanto de redes internas catalogadas como seguras, así como intentos de acceso provenientes de internet, o redes internas que no hagan parte del alcance.

Figura 14**.** Topología acorde a requisito 1.3.7 de la norma PCI DSS



Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

- **Numeral PCI DSS 1.3.8** No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

Recomendación: A fin de no divulgar la información de direccionamiento IP real de la red, se debe hacer uso de configuraciones ya sea tipo NAT “network address transalation” sobre firewall las cuales permiten hacer traslaciones de direccionamiento IP sobre el tráfico que fluye entre redes confiables y redes no confiables, o se puede utilizar la opción de implementar un proxy para tráfico HTTP, HTTPS y FTP, este toma las conexiones provenientes de la red interna y las envía hacia el destino con la dirección IP propia del proxy configurada para tal fin, tanto la configuración de NAT sobre firewall como la implementación de un servidor proxy tienen como fin mantener en secreto el direccionamiento IP real de los equipos que hacen parte del alcance PCI DSS y puede ser implementado cualquiera de los dos métodos o los dos según sea el caso teniendo en cuenta que la solución proxy aplica sólo para protocolos HTTP, HTTPS y FTP.

Para mayor detalle de cómo realizar configuración de NAT “network address translations” diríjase a la URL https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf página en la página 114 sección 2.8.5. “FORWARD and NAT Rules”

- **Numeral PCI DSS 7.2** Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para “negar todo”, salvo lo que se permita específicamente.

Recomendación: Una mejor práctica en la configuración de un firewall es negar todo y aceptar sólo los accesos que sean explícitamente necesarios, para ello se debe crear una regla configurada de la siguiente forma:

- IP origen any
- IP destino any
- Servicio o protocolo any
- Acción denegar

Una vez establecida la regla de denegación arriba de esta se debe iniciar con la configuración de las reglas acorde a las necesidades del negocio como lo son reglas de correo entrante y saliente, reglas de servidores WEB, regla para interacción de aplicaciones entre los diferentes segmentos de red, reglas de administración de aplicaciones y software base entre otros.

- **Numeral PCI DSS 7.2.1** Cobertura de todos los componentes del sistema.

Recomendación: Para efectos de administración de firewall se debe contar con un segmento de red exclusivo para tal fin y este segmento debe estar protegido y las reglas de acceso deben estar configuradas de tal forma que sólo permitan los accesos de los administradores con los servicios o protocolos propios para realizar estas funciones, un ejemplo de una regla es:

- IP origen “IP del computador del administrador firewall” ejemplo 192.168.1.10/32

- IP destino “IP del segmento de administración del firewall” ejemplo 192.168.2.1/32

- Servicio o protocolo SSH, HTTPS.

- Acción permitir

Con la configuración anterior se permite sólo al administrador del firewall llegar al segmento de administración del mismo con el fin de realizar labores de administración, cambio de configuración, aplicación de parches de seguridad.

- **Numeral PCI DSS 7.2.3** Configuración predeterminada de “negar todos”.

Recomendación: Acorde al numeral 7.2 la configuración firewall se debe establecer de tal forma que se nieguen todos los accesos y se deben permitir exclusivamente los accesos necesarios y estos deben estar acordes a las necesidades del negocio, ver regla de configuración denegar todo en numeral 7.2.

- **Numeral PCI DSS 12.10.5** Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

Recomendación: Los logs generados a partir de las reglas de configuración en firewall, deben redirigirse a herramientas de monitoreo para realizar seguimiento a los accesos provenientes de redes no confiables hacia segmentos de red que hace parte del alcance PCI DSS, esta redirección puede realizarse a través del servicio syslog o a través de correo definiendo reglas para el envío de alertas ante ciertas situaciones específicas como la presentada cada vez que se realiza un acceso a la consola de administración firewall.

5.4.2 Filtrado de contenido. Para esta herramienta se escogió el software SQUID, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la 3.5.10, (fecha de revisión, 5 de octubre de 2015).http://www.squid-cache.org/Versions/.

- Documentación y configuración de SQUID.
http://www.squid-cache.org/Doc/

- Configuration en Linux Centos.
http://www.alcancelibre.org/staticpages/index.php/19-0-como-squid-general

- Configuration en Linux Debian.
https://www.lisenet.com/2014/install-and-configure-squid3-caching-proxy-on-debian-wheezy/

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

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

Recomendación: Es necesario garantizar que ningún activo del entorno PCI DSS cuente con salida directa hacia internet, para esto es necesario implementar un proxy el cual debe hacer frente a las conexiones salientes hacia Internet, una de las mejores formas de implementar un proxy es configurarlo de modo explícito, para mayor información consultar la URL http://www.deckle.co.uk/squid-users-guide/browser-configuration.html , sección “Basic Configuration”, configurando el proxy de este modo se enruta a través de él, todo el tráfico que sale y entra hacia y desde internet, ver figura 1.6 Topología Proxy.

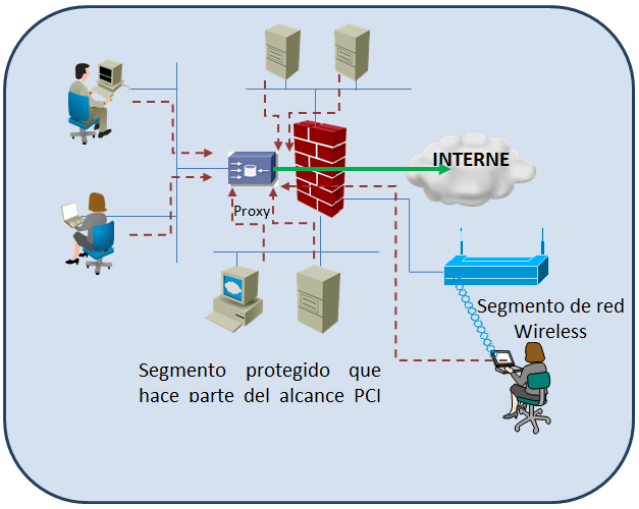
- **Numeral PCI DSS 1.3.3** No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y el entorno del titular de la tarjeta.

Recomendación: Remitirse a la recomendación dada en el numeral PCI DSS 1.3 para la herramienta proxy SQUID.

- **Numeral PCI DSS 1.3.8** No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.

Recomendación: A fin de no divulgar la información de direccionamiento IP real de la red, se debe implementar un proxy en modo explícito para el tráfico saliente HTTP, HTTPS y FTP , este toma las conexiones provenientes de la red interna y las envía hacia el destino con la dirección IP propia del proxy configurada para tal fin, esta implementación tiene como fin mantener en secreto el direccionamiento IP real de los equipos que hacen parte del alcance PCI DSS Para mayor detalle de cómo realizar configuración remítase a http://www.deckle.co.uk/squid-users-guide/squid-configuration-basics.html , ver figura 15 Topología Proxy.

Figura 15. Topología Proxy



Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

5.4.3 IPS. Para esta herramienta se escogió el software SNORT, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la snort-2.9.7.6, (fecha de revisión, 5 de octubre de 2015).https://www.snort.org/downloads**,** de igual forma puede consultar documentación de la herramienta enhttps://www.snort.org/documents.

- Configuración de SNORT en Linux Centos.
https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/070/original/snort-centos6x-7x-rev1.pdf.

- Configuración de SNORT en Linux Debian.
https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/049/original/Debian___Snort_based_Intrusion_Detection_System.pdf .

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 11.1** Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados.

Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.

- **Numeral PCI DSS 11.4** Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos.

Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.

Recomendación: Dado que los IPS´s están en capacidad de hacer validaciones a nivel de red y de aplicación para detección y prevención de ataques, se debe

disponer de protección IPS para los segmentos que hacen parte del alcance PCI DSS, típicamente y al menos se deben considerar los segmentos de red en donde se encuentran conectados servicios como internet, DMZ, aplicación y bases de datos.

Para cada segmento de red a proteger se debe disponer de una política acorde a los activos a proteger, es decir si sobre la red DMZ se encuentran sólo servidores con sistema operativo Linux y con servicios para publicación de páginas WEB mediante apache, no tiene sentido tener activas firmas de detección de intrusos para otros sistemas operativos como Windows o AIX, tampoco se deben activar firmas para detección de aplicaciones para publicar sitios WEB como Internet Information Services “IIS”.

Para el caso del segmento de red DMZ el cual cuenta con servidores con sistema operativo Linux y servicios de publicación WEB con apache, las firmas configuradas sobre el IPS para protección de este segmento de red deben estar asociadas al sistema operativo y aplicativo que se encuentre activo sobre el o los servidores a proteger, de esta forma se consigue un mejor rendimiento del IPS al no tener que analizar firmas que no son acordes a activos a proteger, por otro lado se disminuye sustancialmente el número de falsos positivos lo cual permite un mejor análisis de los eventos detectados por el IPS.

Con el fin de mantener actualizadas las firmas del IPS consulte la página del fabricante https://www.snort.org/products , allí encontrará la información necesaria para obtener las firmas actualizadas de esta herramienta.

5.4.4 NTP. Para esta herramienta se escogió el software NTP bajo sistema operativo LINUX, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la 4.2.8p3, (fecha de revisión, 5 de octubre de 2015). http://www. ntp.org/downloads.html, de igual forma puede consultar documentación de la herramienta en NTP enhttp://www.ntp.org/documentation.html.

- Configuración de NTP en Linux Centos. http://www.alcancelibre.org/static pages/index.php/como-ntp .

- Configuración de NTP en Linux Debian. http://man-es.debianchile.org/ntp.html .

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 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.

Con el fin de mantener una hora uniforme sobre todos los dispositivos que hacen parte del alcance PCI DSS es necesario contar con un servidor NTP el cual sirva para tal fin, este servidor NTP debe sincronizar su base de tiempo a través de la hora legal colombiana, para ello se debe tomar como base de tiempo con http://horalegal.inm.gov.co/ .

- **Numeral PCI DSS 10.4.1** Los sistemas críticos tienen un horario uniforme y correcto.

- **Numeral PCI DSS 10.4.3** Los parámetros de la hora se reciben de fuentes aceptadas por la industria.

Recomendación: Dado que el servicio NTP se torna de gran importancia a la hora de mantener referencia horaria en logs de sistema y transaccionales es conveniente contar con dos servidores NTP a fin de mantener la hora sincronizada en caso de falla de alguno de los servidores.

5.4.5. DLP. Para esta herramienta se escogió el software OpenDLP, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma.

- Descarga de software Open DLP, tener en cuenta la última versión estable, para este caso es la 0.51, (fecha de revisión, 14 de diciembre de 2015). Standalone: https://code.google.com/p/opendlp/downloads/list.

- Instalación y configuración de Open DLP. Standalone: http://opendlp.google code.com/files/README-0.5.1

A continuación, se expondrá el punto de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 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.).

Recomendación: Al implementar una herramienta de prevención de pérdida de datos DLP se debe tomar en cuenta las siguientes recomendaciones:

- Las herramientas de prevención de pérdida de datos DLP no son 100% efectivas, por eso su nombre lo específica “prevención” por eso importante al momento de implementar tener en cuenta que es necesario realizar afinamiento y actualizaciones periódicas a este tipo de herramientas, a fin de lograr el mayor porcentaje de efectividad posible.

- Para implementar un DLP enfocado a prevenir perdida de datos de tarjetas de crédito es necesario en lo posible que la herramienta este en la capacidad de analizar el algoritmo LUHN, este algoritmo fue diseñado para calcular y validar números de tarjetas e IMEI de teléfonos celulares, si requiere información adicional puede dirigirse al siguiente enlace: http://isecauditors.com/ sites/default/ files//files/RedSeguridad_49_Tokenizacion.pdf

En la mayoría de los casos no es suficiente con instalar la herramienta DLP sobre el activo en sí, es necesario además contar con una herramienta de DLP en el perímetro, un DLP perimetral ayuda a fortalecer la estrategia de prevención de fuga de información sensible, ya que se convierte en un chequeo adicional y que tiene la capacidad de analizar otros tipos de tráfico (HTTP, NET BIOS, IRC) que el DLP de host no logra analizar.

5.4.6 Descubrimiento de datos de tarjeta. Para esta herramienta se escogió el software CCSRCH, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma.

- Descarga de software CCSRCH, tener en cuenta la última versión estable, para este caso es la 1.0.8, (fecha de revisión, 14 de diciembre de 2015). https://github. com/adamcaudill/ccsrch.

- Instalación y configuración de CCSRCH. https://github.com/adamcaudill/ ccsrch.

A continuación, se expondrá el punto de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 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.).

Recomendación: Para implementar herramienta de descubrimiento de datos de tarjetas de crédito tenga en cuenta:

La norma no especifica el método de ejecución de estos descubrimientos, por lo que una buena práctica es parametrizar el descubrimiento a las unidades de los activos en donde se tenga certeza de la existencia de datos de tarjeta y que estos hagan parte del alcance, lo anterior con el fin de lograr una optimización en el tiempo de ejecución del proyecto y disminuir el impacto sobre el procesamiento de los activos a monitorear, para los activos que no hacen parte del alcance es necesario realizar el descubrimiento sobre todas las unidades de almacenamiento disponibles.

Es necesario iniciar el despliegue de la herramienta y la ejecución de los descubrimientos en activos de pruebas, a fin de poder determinar un patrón de comportamiento para posteriormente desplegar en producción.

Si los activos hacen parte del núcleo de la operación la recomendación es monitorear el activo durante todo el proceso de ejecución, ya que este tipo de herramientas puede generar archivos temporales de gran tamaño que pueden llegar a llenar la capacidad de almacenamiento de los discos duros y de esta manera afectar el desempeño del activo.

5.4.7 Firewall de aplicación (WAF). Para esta herramienta se escogió el software MOD Security, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la v2.9.0, (fecha de revisión, 14 de diciembre de 2015). https://www.modsecurity.org/download.html.

- Instalación y configuración de MOD Security. https://github.com/Spider Labs/ModSecurity/wiki/Reference-Manual.

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 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 con 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.

Nota: Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2.

Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.

- **Numeral PCI DSS 12.10.5.** Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

Recomendación: A la hora de implementar una solución WAF es necesario tener en cuenta los siguientes aspectos:

Contar con los certificados digitales necesarios para que la aplicación WEB a proteger funcione de forma correcta, estos deben ser importados al WAF ya que este estará al frente de las peticiones que los clientes realicen.

El WAF realiza labores de descifrado de los paquetes con el fin de realizar inspecciones en búsqueda de tráfico malicioso, en el caso en el que el WAF no pueda realizar la labor de descifrado del tráfico proveniente del cliente, el acceso a la aplicación no funcionará.

5.4.8 Monitoreo de integridad de archivos. Para esta herramienta se escogió el software OSSEC, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software, tener en cuenta la última versión estable, para este caso es la 2.8.3, (fecha de revisión, 14 de diciembre de 2015). http://ossec.github.io/downloads.html.

- Instalación y configuración de OSSEC. http://ossec.github.io/docs/manual/ index.html.

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 10.5.5** Utilice el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen.

- **Numeral PCI DSS 11.5** Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de monitorización de integridad de archivos).

- **Numeral PCI DSS 12.10.5** Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.

Recomendación: Para implementar herramienta de monitoreo de integridad de archivos OSSEC tenga en cuenta:

La herramienta OSSEC aun cuando cuenta con una consola centralizada, el despliegue debe realizarse activo por activo a ser monitoreado, el servidor principal genera una llave única la cual debe ingresarse en cada activo, esto es una importante consideración en los tiempos de planeación si se cuenta con un número considerable de activos.

Es necesario definir las rutas críticas a monitorear en la herramienta, es decir que adicional a las rutas del sistema operativo se debe definir las rutas de las aplicaciones que funcionan sobre los activos monitoreados a fin de detectar cualquier alteración en la integridad de las configuraciones de las herramientas.

5.4.9 Antivirus. Si bien es cierto que existen herramientas libres que prestan una solución al problema de los virus, también es necesario considerar que ninguna de ellas cumple con la totalidad de los requisitos exigidos por la …norma PCI DSS V 3.0…, especialmente en los …numerales 5.2 y 5.3… los cuales solicitan explícitamente que el software de antivirus se debe mantener actualizado a diario y generar los de auditoría con tiempos de retención de por lo menos un año, adicionalmente esta gestión debe realizarse desde una consola centralizada, y es ahí específicamente en donde ninguna herramienta de software libre cumple, adicionalmente también se exige que el motor de anti virus no pueda ser manipulado por los usuarios, debido a los puntos anteriormente expuestos no es recomendable la implementación de ninguna herramienta antivirus de software libre para el cumplimiento de la norma PCI DSS V 3.0.

A continuación, se expone cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento

- **Numeral PCI DSS 5.1** Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).

- **Numeral PCI DSS 5.1.1** Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.

- **Numeral PCI DSS 5.2** Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente:

  - Estén actualizados.

  - Ejecuten análisis periódicos.

  - Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.

- **Numeral PCI DSS 5.3** Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado.

Recomendación**:** debido a que no se encontró ninguna herramienta libre que cumpla con todos los requisitos PCI DSS versión 3.0 no se recomendara ningún software específico. Sin embargo, es de tener en cuenta que en la actualidad las casas de software más grandes están orientando sus mercados a las pequeñas empresas. Por lo cual, han creado soluciones especiales muy competitivas para microempresas a un costo relativamente bajo y que cumplen con los requisitos de la norma en cuanto a antivirus.

5.4.10. Cifrado de datos. Para esta herramienta se escogió el software IPSEC Libreswany LUKS, a continuación, se relacionan los sitios en los cuales puede consultar información acerca de la descarga del software, documentación general de la herramienta y configuración de la misma:

- Descarga de software IPSEC Libreswan, tener en cuenta la última versión estable, para este caso es la 3.15, (fecha de revisión, 14 de diciembre de 2015).https://download.libreswan.org/.

- Instalación y configuración de IPSEC Libreswan.
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html#sec-Securing_Virtual_Private_Networks.

- Instalación y configuración de LUKS.
http://www.alcancelibre.org/staticpages/index.php/ciframiento-particiones-luks.

A continuación, se expondrá cada uno de los puntos de la norma brindando una explicación técnica, con el fin de ayudar a su interpretación, y así lograr su respectivo cumplimiento:

- **Numeral PCI DSS 2.2.3** Implemente funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSEC VPN, para proteger los servicios no seguros, como NetBIOS, archivos compartidos, Telnet, FTP, etc.

- **Numeral PCI DSS 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 otros tipos de acceso administrativo que no sea de consola.

- **Numeral PCI DSS 3.4.1** Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios.

- **Numeral PCI DSS 3.6.2** Distribución segura de claves de cifrado.

- **Numeral PCI DSS 3.6.3** Almacenamiento seguro de claves de cifrado.

- **Numeral PCI DSS 3.6.6** Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido.

- **Numeral PCI DSS 4.1** Utilice cifrado sólido y protocolos de seguridad (por ejemplo, SSL/TLS, IPSEC, SSH, etc.) para proteger los datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas, como, por ejemplo, las siguientes:

  - Solo se aceptan claves y certificados de confianza.
  - El protocolo implementado solo admite configuraciones o versiones seguras.

  - La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza.

  - Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes:

- La Internet
- Tecnologías inalámbricas, incluso 802.11 y Bluetooth
- Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código)
- Servicio de radio paquete general (GPRS)
- Comunicaciones satelitales

- **Numeral PCI DSS 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.).

Recomendación: Para implementación de funcionalidades de cifrado es importante tener en cuenta:

- Tamaño de las llaves usadas para labores de cifrado, como mínimo se deben usar llaves de 256 bytes.

- Uso de algoritmos de validación de integridad de datos robustos, se deben usar algoritmos de validación de integridad de datos como SHA2, no se debe hacer uso de algoritmo de verificación de integridad MD5 ya que este es considerado inseguro.

- La lista de algoritmos declarados como seguros o inseguros pueden ser revisada en la siguiente URL de la página NIST, http://csrc.nist.gov/groups/STM/cavp/validation.html.

CONCLUSIONES

- La investigación demuestra que la implementación de la norma con la herramienta comercial líder o con las que están incursionando en este mercado, tiene un valor considerable como se puede observar en el cuadro 32. Esta investigación se originó de acuerdo a los costos que representa la implementación de la norma para las PYMES y la posibilidad de implementarla con herramientas libres. Se puede observar en el cuadro 32 que se reducen los costos drásticamente con herramientas libres, por lo cual la presente investigación se convierte un documento de gran valor para las PYMES que necesitan saber cuál son las mejores herramientas libres para implementar la norma PCI-DSS V 3.0.

Cuadro 32**.** Comparativo de costos de inversión e implementación de herramientas de seguridad para cumplimiento de requisitos tecnológicos PCI DSS V 3.0

Herramientas De Seguridad	**Valor de Inversión**		
	Software comercial líder	**Software comercial incursionando en mercado**	**Software libre**
Firewall de red	$97’742.950	$ 66’420.000	$21.236.000
Intrussion prevention system (IPS)	$208’702.500	$155’000.000	$ 13’148.047
Network time protocol (NTP)	$8’000.002	$8’500.000	$4’000.002
Filtro de contenido	$186’500.000	$50’887.500	$ 13’148.047
Data loss prevention (DLP)	$61’698.500	$63’354.750	$ 21’236.000
Descubrimiento de datos de tarjeta	$0	$0	$0
Web application firewall (WAF)	$199’324.000	$ 178’446.001	$ 14’148.047
Monitoreo de integridad de archivos	$59’048.500	$47’773.500	$21’236.000
Escanner de vulnerabilidades	$49’173.500	$43’861.000	$26’236.000
Antivirus	$7’222.426	$7’745.615	$1’500.000
Cifrado de datos	$8´531.698	$30´048.930	$2´000.000
TOTAL	**$885’944.076**	**$652’037.296**	**$137’888.143**

Fuente: Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

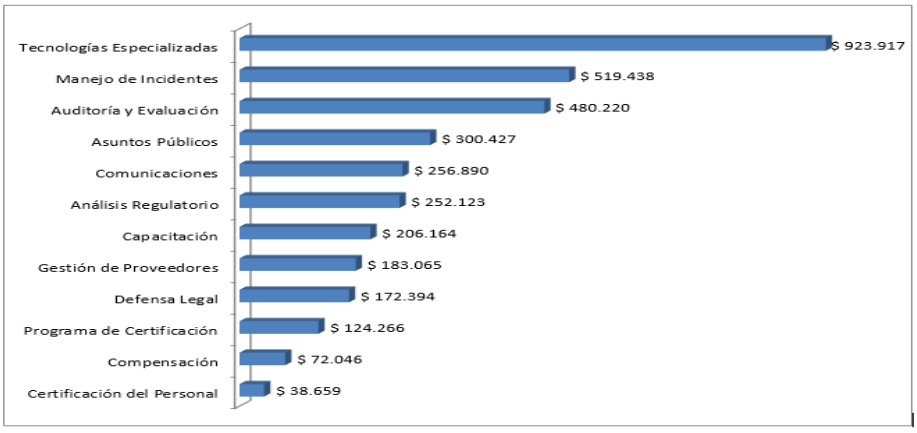
- Las herramientas libres son de gran utilidad para casos en los que no se cuenta con presupuesto para adquirir software comercial, y si bien es cierto que las soluciones basadas en tecnologías de software libre representan costos

relativamente menores, también requieren en la mayoría de los casos una mayor administración y capacitación para su operación, adicional a que es complejo el soporte debido a que no es fácil conseguir especialistas en estas herramientas y el soporte generalmente es basado en manuales y foros de ayuda.

- Las herramientas libres propuestas en el presente documento a excepción del antivirus cumplen con los requisitos de la norma, sin embargo estas deben ser configuradas de forma adecuada, por lo cual la implementación de herramientas tecnológicas exigidas por la norma PCI DSS, debe acogerse a estándares de endurecimiento de su configuración, mantenerse actualizada y libre de brechas de seguridad conocidas y mitigadas por el fabricante, contar con administración y documentación, junto con un constante análisis de riesgo de la plataforma, todo ello con el fin de mantener los requisitos de cumplimiento de la norma PCI DSS, ya que se podría implementar la mejor herramienta ya sea comercial o libre pero si esta no es parametrizada o configurada de forma adecuada no se podrá dar cumplimiento a los puntos de la norma.

- La inversión tecnológica de protección de datos es considerablemente alta para la implementación de la norma PCI DSS V 3.0, seguida del manejo de incidentes, estas dos categorías representan los gastos más grandes del proceso de cumplimiento PCI DSS, aunque lo anterior no significa que sean las únicas inversiones, como se puede observar la Figura 10.se pueden evidenciar otros costos asociados a temas como capacitación, auditorías, análisis regulatorio entre otros, y estos se encuentran expresados en dólares y corresponde al promedio de 46 compañías multinacionales según reporte del Ponemon Institute The True cost of Compliance.

Figura 16. Costos de cumplimiento PCI por categoría de gasto



Fuente Ponemon Institute. The true cost of compliance. [En línea]. <http://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf>

BIBLIOGRAFÍA

AESCRYPT. AES. Crypt Documentation. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.aescrypt.com/documentation/>

ALTONIVEL. Los 10 hackers más famosos del mundo. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.altonivel.com.mx/los-10-hackers-mas-famosos-del-mundo.html

ARANDA SOFTWARE. Aranda 360. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://arandasoft.com/aranda-360/

AYUSO NEIRA, Pablo. Licensing Information about net filter/iptables. [en línea], [consultado el 15 de Junio del 2015]. Disponible en; <http:// www.netfilter. org/licensing.html>

BALCÁZAR, Priscila. Todo lo que necesita saber sobre PCI (PaymentCardIndustry Security Standards) y no se atrevía a preguntar. [En línea]. [consultado el 15 de junio de 2015]. Disponible en: http://www.magazcitum.com.mx/?p=59

BRADLEY Martin, DENT W. Alexander. Payment Card Industry Data Security Standard (PCI DSS) – What it is and its impact on retail merchants. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://cdn.ttgtmedia. com/searchSecurityUK/downloads/RHUL_Bradley_ 2010.pdf>

CAUDILL. CCSRCH - Open Source PAN / Credit Card Scanner. [En línea]. [citado el 15 de Junio del 2015]. Disponible en: http://adamcaudill.com/ccsrch/>

CHECK POINT. Endpoint Remote Access VPN. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.checkpoint.com /products/endpoint-remote-access-vpn-software-blade/>

CLAMAV. CLAM. AntiVirus 0.98. User Manual. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <https://github.com/vrtadmin/clamav-faq/raw/ master/ manual/clamdoc.pdf>

CÓMODO. CÓMODO. Endpoint Security Manager (ESM). [En línea], [consultado el 15 de Junio del 2015]. Disponible en: https://www.comodo.com/business-enterprise/endpoint-protection/endpoint-security-manager.php

CONSEJO DE ESTÁNDARES DE SEGURIDAD PCI O PCI. Oversight and History.[En línea]. [consultado el 15 de Junio del 2015], Disponible en: <http://www.focusonpci.com/ site/index.php/ pdf/About-PCI/pci-oversight-and-history.pdf>

CONTROLCASE. Software de Descubrimiento de Datos para Tarjetas de Crédito y Datos de los Tarjetahabientes para PCI DSS. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://www.controlcase.com/es/data_discovery.php

CRIMESSYSTEMS. Cuál es la historia de los delitos informáticos. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://crimes systems.blogspot.es/>

DELL. Soluciones para necesidades empresariales PCI-DSS Compliance. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www. sonicwall.com/es/es/solutions/Solutions-PCI-Compliance.html#tab=bestpractices>

DEVICELOCK TECHNOLOGY. Prevent Devastating Data Leaks by Securing the Endpoints of Your Network. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.devicelock.com/products/>

FINANZAS Y BANCA. Hacia una estrategia consolidada para el cumplimiento de la normativa PCI DSS. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: http://www.finanzasybanca.com/index.php/hacia-una-estrategia-consolidada-para-el-cumplimiento-de-la-normativa-pci-dss.html>.

FUNDACIÓN GNU. Donar hardware de computadora es también **útil** en ocasiones, [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://gnu.ist.utl.pt/help/donate.es. html#HowIndividualsCanDonate>

GARTNERT, INC. investigación y análisis para las industrias. [En línea] [Consultado el 15 Junio de 2015] http://www.bnamericas.com/company-profile/es/gartner-inc-gartner.

INOCREDITO. Certifíquese en PCI. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.incocredito.com.co/index.php/para-establecimientos - comerciales/ icomo afiliarse/ certifiquese-en-pci.html

INTERNET SECURITY AUDITORS. Implantation y certification en el estándar PCI DSS. [En línea]. < http://www.isecauditors.com/implantacion-pci-dss> [citado el 15 de Junio del 2015]

MCAFEE.MCAFEE Complete Data Protection. [En línea], [consultado el 23 de diciembre de 2015]. Disponible en: http://www.mcafee.com /es/products/complete-data-protection.aspx#vt=vtab-CaracterC3ADsticasyventajas

MCAFEE.SECURITY Management. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.mcafee.com/us/products/security-management/ index.aspx>

_____. Protection Essential for SMB. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <http://www.shopmcafee.com.co/store/mfesmb/es_MX/pd/ThemeID. 36633 000/productID.306911700/categoryID.66300000>

MICROSOFT. ¿Qué es un servidor proxy? [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: http://windows.microsoft.com/es-co/windows-vista/what-is-a-proxy-server>

MUNDOFOX. Vicepresidente de Target inicia audiencia tras escándalo por perdida de información de clientes. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.noticiasmundofox.com/noticias/vicepresidente-de-target-inicia-audiencia-tras-escandalo-por-perdida-de-informacion-de

OPENDLP – FREE & OPEN-SOURCE. Pérdida libre y de código abierto de datos prevención de herramientas. [en línea]. [consultado el 15 de junio del 2015]. disponible en: http://www. darknet.org. uk/2010/05/opendlp-free-open-source-data-loss-prevention-dlp-tool/

OWASP.WEB. application firewall. [en línea], [consultado el 15 de Junio del 2015]. Disponible en: https://www.owasp.org/index.php/Web_Application_ Firewall

PCI Oversight and History. [Enlínea], [consultado el 23 de noviembre de 2015]. Disponible en: http://www.focusonpci.com/site/index.php/pdf/About-PCI/pci-oversight-and-history.pdf

PCI SECURITY STANDARDS COUNCIL. Requisitos de las PCI PA-DSS y procedimientos de evaluación de seguridad, versión 3.0 Noviembre 2013. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf>

_____. Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, [En línea]. [consultado el 23 de noviembre de 2015].disponible en: <https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/ minisite/en/ docs /PCI_DSS_v3_ Glossary_ES-LA.pdf>.

PRIVACY RIGTHS CLEARINHOUSE. Privacidad Derechos de la Cámara de Compensación (PRC) [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://www.privacyrights.org/>

SANS INSTITUTE. A Design for Building an IPS Using Open Source Products. [En línea], [consultado el 15 de Junio del 2015]- Disponible en: <http://www.sans. org/reading-room/whitepapers/intrusion/design-building-ips-open-source-products-1662>

SYMANTEC. Symantec Data Loss Prevention. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.symantec.com/es/mx/data-loss-prevention/>

TECHNET MICROSOFT. Guía de planeación para el cumplimiento del Estándar de seguridad de datos en la industria de tarjetas de pago. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://technet.microsoft.com/es-es/library/bb821241.aspx>

THE GUARDIAN PROJECT. LUKS: Disk Encryption. [En línea], [consultado el 15 de Junio del 2015]. Disponible en: <https://guardianproject.info /code/luks/>

VISA. Seguridad de los datos. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: <http://www.visaeurope.es/visa-para-comercios/seguridad/ seguridad- de-los-datos>

WIKIPEDIA. Network Time Protocol. [En línea]. [consultado el 15 de Junio del 2015]. Disponible en: http://es.wikipedia.org/wiki/Network_Time_Protocol.

WIKIPEDIA DATA. Loss prevention software. [En línea], [citado el 15 de Junio del 2015]. Disponible en: http://en.wikipedia.org/wiki /Data_loss_prevention_software

ANEXOS

Anexo A. Cruce tecnología versus cumplimiento de la norma PCI- DSS V3.0[110]

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas											
1.1 Establezca e implemente normas de configuración para firewalls y routers 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 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.											
1.1.3 El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.											
1.1.4 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.	√										
1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.											
1.1.6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros. Entre los servicios, protocolos o puertos inseguros, se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP versión 1 y versión 2.											
1.1.7 Requisito de la revisión de las normas de firewalls y routers, al menos, cada seis meses.											
1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas. Nota: Una “red no confiable” es toda red externa a las redes que pertenecen a la entidad en evaluación o que excede la capacidad de control o administración de la entidad.	√										
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.	√										
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, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	√										
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 una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.	√										

[110] Los Autores Guía de implementación de herramientas tecnológicas dirigida a las PYMES para dar cumplimiento a la norma internacional PCI DSS v3.0

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la 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 Implementar medidas anti suplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna).	√										
1.3.5 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en 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 del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables	√										
1.3.8 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas. Nota: Entre los métodos para ocultar direcciones IP, se pueden incluir, a modo de ejemplo, los siguientes: • Traducción de Dirección de Red (NAT) • Ubicación de los servidores que contengan datos del titular de la tarjeta detrás de los servidores proxy/firewalls. • Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas, • Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas.	√			√							
1.4 Instale software de firewall personal en todos los dispositivos móviles o de propiedad de los trabajadores que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder a la red. Las configuraciones de firewalls incluyen lo siguiente: • Los parámetros específicos de configuración se definen para cada software de firewall personal. • El software de firewall personal funciona activamente. • Los usuarios de dispositivos móviles o de propiedad de los trabajadores no pueden alterar el software de firewall personal.											
1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores											
2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
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 TODOS los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica al momento de la instalación, incluidas, a modo de ejemplo, las claves de cifrado inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias SNMP (protocolo simple de administración de red).											
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 OrganizationforStandardization (ISO) • SysAdminAudit Network Security (SANS) Institute • NationalInstitute 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). Nota: Cuando se utilicen tecnologías de virtualización, implemente solo una función principal por componente de sistema virtual.											
2.2.2 Habilite solo los servicios, protocolos y daemons, etc., necesarios, según lo requiera la función del sistema.											
2.2.3 Implemente funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros; por ejemplo, utilice tecnologías seguras, como SSH, S-FTP, SSL o IPSec VPN, para proteger los servicios no seguros, como NetBIOS, archivos compartidos, Telnet, FTP, etc.								√			
2.2.4 Configure los parámetros de seguridad del sistema para evitar el uso indebido.											
2.2.5 Elimine todas las funcionalidades innecesarias, 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 otros tipos de acceso administrativo que no sea de consola.								√			
2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS.											
2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
2.6 Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el Anexo A: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados											
3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta): • 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 trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida.						√					
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización. Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos de autenticación confidenciales en los siguientes casos: • Si existe una justificación de negocio. • Si los datos se almacenan de forma segura. 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 (número de cuenta principal) cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver el PAN (número de cuenta principal) completo. Nota: Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
3.4 Convierta el PAN (número de cuenta principal) en 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 del PAN completo) • Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) • Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). • Criptografía sólida con procesos y procedimientos asociados para la administración de claves. Nota: Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN (número de cuenta principal), se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.											
3.4.1 Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios.								√			
3.5 Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido: Nota: Este requisito también se aplica a las claves utilizadas para cifrar los datos del titular de la tarjeta almacenados y para las claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos; dichas claves de cifrado de claves deben ser, al menos, tan seguras como las claves de cifrado de datos.											
3.5.1 Restrinja el acceso a las claves criptográficas a la menor cantidad de custodios necesarios.											
3.5.2 Siempre guarde las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. • Dentro de un dispositivo criptográfico seguro (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). • Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria. Nota: No es necesario guardar las claves públicas de esta manera.											
3.5.3 Guarde las claves criptográficas en la menor cantidad de ubicaciones posibles.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
3.6 Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta, incluso lo siguiente: Nota: Varias normas de la industria relativas a la administración de claves están disponibles en distintos recursos incluido NIST, que puede encontrar en http://csrc.nist.gov.											
3.6.1 Generación de claves de cifrado sólido.								√			
3.6.2 Distribución segura de claves de cifrado.								√			
3.6.3 Almacenamiento seguro de claves de cifrado.								√			
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 SpecialPublication 800-57).											
3.6.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción 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. Nota: Si es necesario retener las claves de cifrado retiradas o reemplazadas, éstas se deben archivar de forma segura (por ejemplo, utilizando una clave de cifrado de claves). Las claves criptográficas archivadas se deben utilizar solo con fines de descifrado o verificación.											
3.6.6 Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido. Nota: Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.								√			
3.6.7 Prevención de sustitución no autorizada de claves criptográficas.											
3.6.8 Requisito para que los custodios de claves criptográficas declaren, formalmente, que comprenden y aceptan su responsabilidad como custodios de claves.											
3.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
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 los datos confidenciales del titular de la tarjeta durante la transmisión por redes públicas abiertas, como por ejemplo, las siguientes: • Solo se aceptan claves y certificados de confianza. • El protocolo implementado solo admite configuraciones o versiones seguras. • La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes: • La Internet • Tecnologías inalámbricas, incluso 802.11 y Bluetooth • Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código) • Servicio de radio paquete general (GPRS) • Comunicaciones satelitales								√			
4.1.1 Asegúrese de que las redes inalámbricas que transmiten los datos del titular de la tarjeta o que están conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a fin de implementar un cifrado sólido para transmitir y autenticar. Nota: Se prohíbe el uso de WEP como control de seguridad											
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.).					√			√			
4.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 5: Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.											
5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).									√		
5.1.1 Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.									√		
5.1.2 Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que pueden aparecer a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.											
5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: • Estén actualizados. • Ejecuten análisis periódicos. • Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.									√		

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado. Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus.								√		
5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras											
6.1 Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, “alto”, “medio” o “bajo”) a las vulnerabilidades de seguridad recientemente descubiertas. Nota: Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria y en el posible impacto. Por ejemplo, en los criterios para clasificar las vulnerabilidades, se puede tener en cuenta la puntuación base CVSS, la clasificación del proveedor o el tipo de sistema afectado. Los métodos para evaluar las vulnerabilidades y asignar las clasificaciones de riesgo varían según el entorno y la estrategia de evaluación de riesgos de la organización. Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de “alto riesgo” para el entorno. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar “críticas” si suponen una amenaza inminente para el entorno, si afectan los sistemas o si generan un posible riesgo si no se contemplan. Algunos ejemplos de sistemas críticos son los sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta.											
6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. Nota: Los parches de seguridad críticos se deben identificar de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
6.3 Desarrolle aplicaciones de software internas y externas (incluso acceso administrativo a aplicaciones basado en web) de manera segura y de la siguiente manera: • De acuerdo con las PCI DSS (por ejemplo, autenticación y registros seguros). • Basadas en las normas o en las mejores prácticas de la industria. • Incorporación de seguridad de la información durante todo el ciclo de vida del desarrollo del software. Nota: Esto rige para todos los software desarrollados internamente y para todos los software personalizados desarrollados externamente.											
6.3.1 Elimine las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes.											
6.3.2 Revise el código personalizado antes de enviarlo a producción o de ponerlo a disposición de los clientes a fin de identificar posibles vulnerabilidades en la codificación (mediante procesos manuales o automáticos) y que incluya, al menos, lo siguiente: • La revisión de los cambios en los códigos está a cargo de personas que no hayan creado el código y que tengan conocimiento de técnicas de revisión de código y prácticas de codificación segura. • Las revisiones de los códigos deben garantizar que el código se desarrolle de acuerdo con las directrices de codificación segura. • Las correcciones pertinentes se implementan antes del lanzamiento. • La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales a los efectos de tratar las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.											
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 Separe los entornos de desarrollo/prueba de los entornos de producción y refuerce la separación con controles de acceso.											
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 Los procedimientos de control de cambios para implementar los parches de seguridad y las modificaciones en los software deben incluir lo siguiente:											
6.4.5.1 Documentación de incidencia.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.											
6.4.5.3 Verifique que se hayan realizado las pruebas de funcionalidad y que el cambio no impacte negativamente en la seguridad del sistema.											
6.4.5.4 Procedimientos de desinstalación.											
6.5 Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo de software de la siguiente manera: • Capacite a los desarrolladores en técnicas de codificación segura, incluso cómo evitar las vulnerabilidades de codificación comunes y cómo se administran los datos confidenciales en la memoria. • Desarrolle aplicaciones basadas en directrices de codificación seguras. Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.10 eran congruentes con las mejores prácticas de la industria al momento de la publicación de esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASPGuide, SANS CWE Top 25, CERT SecureCoding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.											
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 de “alto riesgo” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS).											
Nota: Los Requisitos 6.5.7 al 6.5.10, que siguen a continuación, rigen para las aplicaciones web y las interfaces de las aplicaciones (internas o externas):											
6.5.7 Lenguaje de comandos entre distintos sitios (XSS).											
6.5.8 Control de acceso inapropiado (como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios).											
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF).											
6.5.10 Autenticación y administración de sesión interrumpidas Nota: El Requisito 6.5.10 se considera la mejor práctica hasta el 30 de junio de 2015 y, a partir de ese momento, se convertirá en requisito											
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 con 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 Nota: Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2. • Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.							√				

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
6.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 7: Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.											
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.											
7.1.1 Defina las necesidades de acceso de cada función, incluso lo siguiente: • Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. • Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.											
7.1.2 Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.											
7.1.3 Asigne el acceso según la tarea, la clasificación y la función del personal.											
7.1.4 Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.											
7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según 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 una persona se basa en la clasificación del trabajo y su función.	√										
7.2.3 Configuración predeterminada de “negar todos”.	√										
7.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 8: Identificar y autenticar el acceso a los componentes del sistema.											
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:											
8.1.1 Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.											
8.1.2 Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación.											
8.1.3 Cancele de inmediato el acceso a cualquier usuario cesante.											
8.1.4 Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.											
8.1.5 Administre las ID que usan los proveedores para acceder, respaldar o mantener los componentes del sistema de manera remota de la siguiente manera: • Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. • Se deben monitorear mientras se usan.											
8.1.6 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
8.1.7 Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.											
8.1.8 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente.											
8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar 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.											
8.2.1 Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida.											
8.2.2 Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos tokens o genere nuevas claves.											
8.2.3 Las contraseñas/frases deben tener lo siguiente: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.											
8.2.4 Cambie la contraseña/frase de usuario, al menos, cada 90 días.											
8.2.5 No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas.											
8.2.6 Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso.											
8.3 Incorpore la autenticación de dos factores para el acceso remoto a la red desde fuera de la red por parte del personal (incluso usuarios y administradores) y todas las partes externas involucradas (que incluye acceso del proveedor para soporte o mantenimiento). Nota: La autenticación de dos factores requiere que se utilicen dos de los tres métodos de autenticación (consulte el Requisito 8.2 para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de dos factores. Los ejemplos de tecnologías de dos factores incluyen autenticación remota y RADIUS (servicio dial-in) con tokens; TACACS (sistema de control de acceso mediante control del acceso desde terminales) con tokens y otras tecnologías que faciliten la autenticación de dos factores.											
8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios, que incluye lo siguiente: • Líneamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Líneamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para no seleccionar contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: • Las ID de usuario genéricas se deben desactivar o eliminar. • No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. • Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema											
8.5.1 Requisitos adicionales para los proveedores de servicios: Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente. Nota: El objetivo de este requisito no es aplicarlo a los proveedores de servicios de hosting compartido que acceden a su propio entorno de hosting, donde se alojan numerosos entornos de clientes. Nota: El Requisito 8.5.1 se considera la mejor práctica hasta el 30 de junio de 2015, y a partir de ese momento, se convertirá en requisito.											
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: • Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. • Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.											
8.7 Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera: • Todo acceso, consultas y acciones de usuario en las bases de datos se realizan, únicamente, mediante métodos programáticos. • Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas en estas. • Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos (no las pueden usar los usuarios ni otros procesos que no pertenezcan a la aplicación).											
8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
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 los sistemas en el entorno de datos del titular de la tarjeta.											
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. Nota: “Áreas confidenciales” hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. No se incluyen las áreas públicas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
9.1.2 Implemente controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público. Por ejemplo, las conexiones de red en áreas públicas y en las que pueden acceder los visitantes se pueden inhabilitar y habilitar solo cuando el acceso a la red se autoriza explícitamente. De forma alternativa, se pueden implementar procesos para asegurarse de que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.											
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.											
9.2 Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes, de la siguiente manera: • Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). • Cambios en los requisitos de acceso. • Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación).											
9.3 Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera: • El acceso se debe autorizar y basar en el trabajo de cada persona. • El acceso se debe cancelar inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, se deben devolver o desactivar.											
9.4 Implemente procedimientos para identificar y autorizar a los visitantes. Los procedimientos deben incluir lo siguiente:											
9.4.1 Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y estarán acompañados en todo momento.											
9.4.2 Se identifican los visitantes y se les entrega una placa u otro elemento de identificación con fecha de vencimiento y que permite diferenciar claramente entre empleados y visitantes.											
9.4.3 Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento. expiration.											
9.4.4 A Se usa un registro de visitantes para llevar una pista de auditoría física de la actividad de los visitantes en las instalaciones, en las salas de informática y en los centros de datos donde se almacenan o se transmiten los datos del titular de la tarjeta. 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 Proteja físicamente todos los medios.											
9.5.1 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 en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.											
9.6 Lleve un control estricto de la distribución interna o externa de todos los tipos de medios y realice lo siguiente:											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
9.6.1 Clasifique los medios para poder determinar la confidencialidad de los datos.											
9.6.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.											
9.6.3 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área segura (incluso, cuando se distribuyen los medios a personas).											
9.7 Lleve un control estricto del almacenamiento y la accesibilidad de los medios.											
9.7.1 Lleve un registro detallado del inventario de todos los medios y lleve a cabo inventarios de los medios, al menos, una vez al año.											
9.8 Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales de la siguiente manera:											
9.8.1 Corte en tiras, incinere o convierta en pulpa los materiales de copias en papel para que no se puedan reconstruir los datos del titular de la tarjeta. Proteja los contenedores de almacenamiento destinados a los materiales que se destruirán.											
9.8.2 Controle que los datos del titular de la tarjeta guardados en medios electrónicos sean irrecuperables para que no se puedan reconstruir.											
9.9 Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones. Nota: Estos requisitos rigen para los dispositivos de lectura de tarjetas que se usan en transacciones (es decir, al pasar o deslizar la tarjeta) en los puntos de venta. El objetivo de este requisito no es aplicarlo a los componentes de ingreso de claves, como teclados de computadoras y teclados numéricos de POS (puntos de ventas). Nota: El Requisito 9.9 se considerará la mejor práctica hasta el 30 de junio de 2015, y a partir de ese momento, se convertirá en requisito.											
9.9.1 Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única											
9.9.2 Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento). Nota: Entre los ejemplos de indicios de que un dispositivo puede haber sido alterado o sustituido, se pueden mencionar accesorios inesperados o cables conectados al dispositivo, etiquetas de seguridad faltantes o cambiadas, carcazas rotas o con un color diferente o cambios en el número de serie u otras marcas externas.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
9.9.3 Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos. La capacitación debe abarcar lo siguiente: • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).											
9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas											
10.1 Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.											
10.2 Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:											
10.2.1 Todo acceso por parte de usuarios a los datos del titular de la tarjeta.											
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 y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.											
10.2.6 Inicialización, detención o pausa de los registros de auditoría.											
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 recursos afectados.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
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. Nota: Un ejemplo de tecnología de sincronización es el NTP (protocolo de tiempo de red).			√								
10.4.1 Los sistemas críticos tienen un horario uniforme y correcto.			√								
10.4.2 Los datos de tiempo están protegidos.											
10.4.3 Los parámetros de la hora se reciben de fuentes aceptadas por la industria.			√								
10.5 Proteja las pistas de auditoría para que no se puedan modificar.											
10.5.1 Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.											
10.5.2 Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.											
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.											
10.5.4 Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.											
10.5.5 Utilice el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).										√	
10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas. Nota: Para cumplir con este requisito, se pueden usar herramientas de recolección, análisis y alerta de registros.											
10.6.1 Revise las siguientes opciones, al menos, una vez al día: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales), o que podrían afectar la seguridad de los CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales). • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección o sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).											
10.6.2 Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.											
10.6.3 Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.											
10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad).											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
10.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.											
11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados. Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.		√									
11.1.1 Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada.											
11.1.2 Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados.											
11.2 Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos). Nota: Se pueden combinar varios informes de análisis para el proceso de análisis trimestral a fin de demostrar que se analizaron todos los sistemas y que se abordaron todas las vulnerabilidades. Es posible que se solicite documentación adicional para verificar que las vulnerabilidades no resueltas estén en proceso de resolverse. Para el cumplimiento inicial de las PCI DSS, no es necesario tener cuatro análisis trimestrales aprobados si el asesor verifica que 1) el resultado del último análisis fue aprobado, 2) la entidad ha documentado las políticas y los procedimientos que disponen la realización de análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En los años posteriores a la revisión inicial de las PCI DSS, debe haber cuatro análisis trimestrales aprobados.											√
11.2.1 Lleve a cabo análisis trimestrales de las vulnerabilidades internas y vuelva a repetir el análisis cuantas veces sea necesario hasta corregir todas las vulnerabilidades de “alto riesgo” (según lo estipulado en el Requisito 6.1). Los análisis deben estar a cargo de personal calificado.											√

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
11.2.2 Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI Security Standards Council). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados. Nota: los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor aprobado de análisis (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). Consulte la Guía del programa de ASV (proveedor aprobado de escaneo) publicada en el sitio web del PCI SSC para obtener información sobre las responsabilidades de análisis del cliente, sobre la preparación del análisis, etc.											
11.2.3 Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado.											
11.3 Implemente una metodología para las pruebas de penetración que incluya lo siguiente: • Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). • Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. • Incluya pruebas del entorno interno y externo de la red. • Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. • Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. • Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. • Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. • Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección. Nota: Esta actualización del Requisito 11.3 se considerará la mejor práctica hasta el 30 de junio de 2015, y a partir de ese momento, se convertirá en requisito. Los requisitos de la versión 2.0 de las PCI DSS para las pruebas de penetración estarán vigentes hasta que se implemente la versión 3.0.											
11.3.1 Lleve a cabo pruebas de penetración externas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
11.3.2 Lleve a cabo pruebas de penetración internas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).											
11.3.3 Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones.											√
11.3.4 Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, realice pruebas de penetración, al menos, una vez al año y después de implementar cambios en los métodos o controles de segmentación para verificar que los métodos de segmentación sean operativos y efectivos, y que aíslen todos los sistemas fuera de alcance de los sistemas dentro del alcance.											
11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.		√									
11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de monitorización de integridad de archivos) para alertar al personal sobre modificaciones no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana. Nota: A los fines de la detección de cambios, generalmente, los archivos críticos son aquellos que no se modifican con regularidad, pero cuya modificación podría implicar un riesgo o peligro para el sistema. Generalmente, los mecanismos de detección de cambios, como los productos de monitorización de integridad de archivos, vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.										√	
11.5.1 Implemente un proceso para responder a las alertas que genera la solución de detección de cambios.											
11.6 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.											
Requisito 12: Mantener una política que aborde la seguridad de la información de todo el personal											
12.1 Establezca, publique, mantenga y distribuya una política de seguridad.											
12.1.1 Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
12.2 Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: • Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.). • Identifica activos críticos, amenazas y vulnerabilidades. • Da lugar a una evaluación de riesgos formal. Los ejemplos de metodologías de evaluación de riesgos incluyen, entre otros, OCTAVE, ISO 27005 y NIST SP 800-30.											
12.3 Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente. Nota: Entre los ejemplos de tecnologías críticas, se incluyen las tecnologías inalámbricas y de acceso remoto, las computadoras portátiles, las tabletas, los dispositivos electrónicos extraíbles, el uso del correo electrónico y de Internet. Asegúrese de que estas políticas de uso requieran lo siguiente:											
12.3.1 Aprobación explícita de las partes autorizadas.											
12.3.2 Autenticación para el uso de la tecnología.											
12.3.3 Lista de todos los dispositivos y el personal que tenga acceso.											
12.3.4 Método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos).											
12.3.5 Usos aceptables de la tecnología.											
12.3.6Ubicaciones 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 Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso.											
12.3.10 En el caso del personal que tiene acceso a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad comercial definida. Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección de los datos de conformidad con los requisitos correspondientes de las PCI DSS.											
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.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
12.5 Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información:											
12.5.1 Establezca, documente y distribuya las políticas y los procedimientos de seguridad.											
12.5.2 Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente.											
12.5.3 Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones.											
12.5.4 Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.											
12.5.5 Monitoree y controle todo acceso a los datos.											
12.6 Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta.											
12.6.1 Capacite al personal inmediatamente después de contratarlo y, al menos, una vez al año. Nota: Los métodos pueden variar según el rol del personal y del nivel de acceso a los datos del titular de la tarjeta.											
12.6.2 Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa.											
12.7 Examine al personal potencial antes de contratarlo 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). Nota: En el caso de los posibles candidatos para ser contratados, como cajeros de un comercio, que solo tienen acceso a un número de tarjeta a la vez al realizar una transacción, este requisito es solo una recomendación.											
12.8 Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera:											
12.8.1 Mantenga una lista de proveedores de servicios.											
12.8.2 Mantenga un acuerdo por escrito en el que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. Nota: La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.											
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios, que incluya una auditoría adecuada previa al compromiso.											
12.8.4 Mantenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.											
12.8.5 Conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
12.9 Requisitos adicionales para los proveedores de servicios: Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. Nota: Este requisito se considerará la mejor práctica hasta el 30 de junio de 2015 y, a partir de ese momento, se convertirá en requisito. Nota: La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.											
12.10 Implemente un plan de respuesta ante incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.											
12.10.1 Desarrolle el plan de respuesta ante incidentes que se implementará en caso de que ocurra una falla 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 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 ante incidentes de las marcas de pago.											
12.10.2 Pruebe el plan, al menos, una vez al año.											
12.10.3 Designe a personal específico para que esté disponible las 24 horas al día, los 7 días de la semana para responder a las alertas.											
12.10.4 Capacite adecuadamente al personal sobre las responsabilidades de respuesta ante fallas de seguridad.											
12.10.5 Incluya alertas de los sistemas de monitorización de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de monitorización de integridad de archivos.	√	√					√			√	
12.10.6 Elabore un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.											
Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas											
A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicios u otra entidad), según los puntos A.1.1 a A.1.4: Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS. Nota: Aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad debe cumplir con las PCI DSS y validar el cumplimiento, según corresponda.											
A1.1 Asegúrese de que cada entidad solo implemente procesos que tengan acceso al entorno de datos del titular de la tarjeta de la entidad.											

ANEXO A. (Continuación)

Requerimientos PCI DSS v3.0	FIREWALL DE RED	IPS	NTP	PROXY FILTRO CONTENIDO	DLP	DESCUBRIMIENTO DE DATOS DE TARJETA	WAF	CIFRADO DE DATOS	ANTIVIRUS	FIM	ESCANER DE VULNERABILIDADES
A.1.2 Limite el acceso y los privilegios de cada entidad solo al entorno de sus propios datos del titular de la tarjeta.											
A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos del titular de la tarjeta de cada entidad y que cumplan con el Requisito 10 de las PCI DSS.											
A.1.4 Habilite los procesos para que se realice una investigación forense oportuna en caso de que un comerciante o proveedor de servicios alojado corra riesgos.											

PCI DSS en Colombia

Javier Perdomo Valderrama
Javier_perdomo_valderrama@hotmail.com
Hugo Alejandro Casallas Larrotta
alejandrohacl@hotmail.com
Julio Alberto Vargas Fernández
julioavargasf@gmail.com
Universidad Piloto de Colombia

Resumen. Día a día el mercado de soluciones de pago electrónico tiene mayores retos y exigencias a nivel de implementación de soluciones de seguridad informática, las franquicias como VISA, Master Card, American Express, exigen la adopción e implementación de la normativa PCI DSS V. 3.0, los costos asociados a la implementación de soluciones tecnológica a fin de dar cumplimiento a los requisitos exigidos por esta norma son bastante altos para ser llevada a cabo por una PIME, debido a esta problemática nacen estrategias basadas en la implementación de soluciones apoyadas en software libre para dar cumplimiento a los requisitos exigidos por la norma con un costo accesible para este tipo de compañías con inversión en tecnología limitada.

I. Qué es PCI DSS V 3.0.

La norma de seguridad de datos PCI DSS v3.0 es un estándar que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito[1].

II. Para qué se usa la norma PCI DSS V 3.0.

La norma internacional PCI DSS en su versión 3.0 vela por salvaguardar la seguridad de los datos de los tarjetahabientes y es exigida a todas las entidades que participan en procesos con tarjetas de pago ya sea en su almacenamiento, procesamiento o transmisión de datos de titulares de tarjeta, lo anterior conlleva a las entidades que deben cumplir con la norma a:

- Asumir altos costos en inversión e implementación de herramientas tecnológicas para dar cumplimiento a requisitos exigidos en la norma PCI DSS 3.0
- Falta de información frente a cómo dar cumplimiento a los requisitos tecnológicos exigido por la norma.
- Altos tiempos de implementación en soluciones tecnológicas.

III. Costos de Implementación de PCI DSS V 3.0.

La implementación de los controles tecnológicos exigidos por la norma PCI DSS V 3.0 a través de herramientas con software licenciado demanda una inversión tecnológica de alrededor de $ 950 millones de pesos, la implementación de estos mismos controles implementando soluciones de software libre requiere de una inversión aproximada de $ 157 millones de pesos, la anterior diferencia

económica apalanca la implementación de la norma para empresas con limitaciones en inversión tecnológica.

A continuación se pueden observar los costos asociados a la implementación de cada herramienta tecnológica licenciada requerida para dar cumplimiento a los requisitos exigidos por la norma PCI DSS.

Cuadro 1. Relación de costos de herramientas tecnológica licenciadas de seguridad.

Herramientas De Seguridad	Valor de Inversión
	Software / Hardware
Firewall de red	$97.742.950
Intrussion prevention system (IPS)	$208.702.500
Network time protocol (NTP)	$8.000.002
Filtro de contenido	$186.500.000
Data loss prevention (DLP)	$61.698.500
Descubrimiento de datos de tarjeta	$61.698.500
Web application firewall (WAF)	$199.324.000
Monitoreo de integridad de archivos	$59.048.500
Escanner de vulnerabilidades	$49.173.500
Antivirus	$7.222.426
Cifrado de datos	$8.531.698
TOTAL	**$947.642.576**

Realizando implementación de las mismas herramientas tecnológicas con software libre se obtiene una reducción de costos de inversión tecnológica de hasta un 85%, a continuación se puede observar los costos asociados.

Cuadro 2. Relación de costos de herramientas tecnológica libre de seguridad.

Herramientas De Seguridad	Valor de Inversión
	Software libre
Firewall de red	$21.236.000
Intrussion prevention system (IPS)	$13.148.047
Network time protocol (NTP)	$4.000.002
Filtro de contenido	$13.148.047
Data loss prevention (DLP)	$21.236.000
Descubrimiento de datos de tarjeta	$20.000.000
Web application firewall (WAF)	$14.148.047
Monitoreo de integridad de archivos	$21.236.000
Escanner de vulnerabilidades	$26.236.000
Antivirus	$1.500.000
Cifrado de datos	$2.000.000
TOTAL	**$157.888.143**

IV. Estado de Adopción de la Norma PCI DSS en Colombia

Colombia está iniciando con la adopción e implementación de la norma PCI DSS, algunos procesadores transaccionales y unos pocos comercios ya han iniciado con esta ardua labor, el caso de Place to Pay, Pagos Online, Credibanco, Redeban Multicolor, Processa, Dispapeles, Hogier, Morpho, Oberthur y PeopleTech, como se puede observar son pocos los comercios y procesadores transaccionales que están trabajando en la implementación de certificación PCI DSS, los costos asociados a la implementación de la norma no son nada alentadores lo que hace que se ofrezca resistencia en su adopción.

V. Conclusión

La implementación de la norma PCI DSS V 3.0 haciendo uso de herramientas de seguridad informática licenciadas tiene un costo asociado bastante alto para ser implementado por una PIME. La posibilidad de adoptar la norma con herramientas de software libre reduce los costos de implementación de una forma drástica lo que posibilita a una PIME invertir en la solución, por lo anterior las implementaciones de soluciones de seguridad informática con software libre se convierten una solución de gran valor para las PYMES con el fin de implementar los controles tecnológicos exigidos por la norma PCI-DSS V 3.0.

Las herramientas libres son de gran utilidad para casos en los que no se cuenta con presupuesto para adquirir software comercial, por otro lado las soluciones basadas en tecnologías de software libre representan menos costos de inversión.

Es necesario tener en cuenta de igual forma que las soluciones de software libre requieren en la mayoría de los casos una mayor administración y capacitación para su operación, adicionalmente es no es fácil contar con soporte debido a la escases de especialistas en este tipo de herramientas y el soporte generalmente es basado en manuales y foros de ayuda.

REFERNCIAS

[1] INTERNET SECUTITY AUDITORS. Implantation y certification en el estandar PCI DSS. [En línea]. < http://www.isecauditors.com/implantacion-pci-dss> [citado el 15 de Junio del 2015]

Javier Perdomo Valderrama
Ingeniero Electrónico Universidad el Bosque
Hugo Alejandro Casallas Larrotta
Ingeniero de Sistemas Universidad Cooperativa de Colombia
Julio Alberto Vargas Fernández
Ingeniero de Sistemas Universidad de Cudinamarca
Aspirantes a Especialización en Seguridad Informática Universidad Piloto de Colombia