

# Automatizar la gestión de vulnerabilidad para el cumplimiento PCI DSS

Una estrategia práctica para la seguridad de la red y el cumplimiento PCI DSS

Este libro blanco identifica los problemas encontrados en la localización de los riesgos de seguridad de red mediante la gestión de vulnerabilidad. Describe como la gestión automatizada de vulnerabilidad contribuye al cumplimiento con los estándares de la industria, como por ejemplo el Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS), y le ayuda en la identificación proactiva de las debilidades de seguridad antes de que sean explotadas.

---

## Introducción

La gestión de vulnerabilidad es una disciplina de administración de riesgo que se encarga de los peligros del comercio electrónico y de los sistemas de información. Puede definirse como el auditoría regular de los componentes hardware y software de infraestructuras de TI, el descubrimiento de debilidades y su resolución. Considerado por muchos Profesionales de TI como un proceso complejo y lento, la gestión de vulnerabilidad es una de las tareas más odiadas y olvidadas de sus cargos.

Sin embargo la gestión de la vulnerabilidad de la red ya no es una opción: Los estándares de la industria como PCI DSS, remarcan consistentemente la importancia de administrar las vulnerabilidades de red y lo exigen como tarea obligatoria en los procesos de cumplimiento.

Este documento trata la necesidad de una gestión eficaz de la vulnerabilidad de red. Describe las molestias y problemas normalmente asociados con este proceso y arroja luz sobre como la automatización puede ayudar a los profesionales de TI a dominar esta disciplina, reducir costes y aumentar los esfuerzos para el cumplimiento PCI DSS.

Introducción .....	2
¿Qué es PCI DSS? .....	2
¿Qué es la gestión de vulnerabilidad de red?.....	3
¿Cuál es la conexión entre PCI DSS y la gestión de vulnerabilidad? .....	4
Los problemas de la gestión de vulnerabilidad .....	5
GFI LANguard Network Security Scanner .....	7
Conclusión.....	7
Acerca de GFI .....	8

---

## ¿Qué es PCI DSS?

PCI DSS es una colección de reglas vinculantes que promueve los procesos de seguridad de TI en las organizaciones que manejan información de pagos con tarjeta. PCI DSS ayuda a reducir el fraude financiero mediante el aumento de las capacidades de seguridad de la red en cualquier procesamiento de información de pago con tarjeta y fue diseñado a causa de 3 factores que alimentan el fraude financiero:

1. Comercio electrónico, que ayuda a superar los límites geográficos y, a menudo, cualquier protección ofrecida por leyes o regulaciones locales.
2. La alta disponibilidad del “dinero de plástico” para las compras del consumidor en todas las naciones industrializadas.
3. Una indiferencia ante las mejores prácticas de seguridad por parte de los negocios que almacenan y/o procesan información no protegida de pagos con tarjeta.

Para contrarrestar el fraude por tarjetas de crédito/débito, las 5 principales empresas de tarjetas (Visa International, MasterCard Worldwide, American Express, JCB y Discover Financial Services) diseñaron un fuerte marco de seguridad para reforzar la seguridad de las transacciones de pagos con tarjeta. El resultado de estos esfuerzos ha sido el Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS). El cumplimiento PCI DSS es responsabilidad irrefutable de todos los negocios que manejan información de titulares de tarjeta incluyendo detallistas, venta por correo, venta por teléfono y comercio electrónico – independientemente del tamaño del negocio.

---

## ¿Qué es la gestión de vulnerabilidad de red?

Las debilidades de seguridad llevan a un flujo continuo de actualizaciones de seguridad emitidas periódicamente por los desarrolladores de soluciones software. Debido a la frecuencia y a la cantidad de actualizaciones de seguridad, los administradores de sistemas encuentran ardua la tarea de mantenerse al día de este proceso. Este abandono permite a los hackers aprovechar sistemas sin parchear y lanzar ataques de red más comúnmente mediante gusanos y virus. Un caso notorio es el gusano Mytob y sus derivados. A pesar del hecho de que Mytob se propaga utilizando vulnerabilidades conocidas para las que existe una solución desde Agosto de 2004, este gusano está todavía activo actualmente y mantiene firmemente la séptima posición en la lista de los 20 virus más activos de Abril de 2007. [Viruslist.com](http://Viruslist.com), [Virus Top 20 for April 2007](#)).

Los ataques dirigidos son también una amenaza cada vez mayor para la continuidad de los negocios cuyos administradores de sistemas deben incluirlo como factor en sus estrategias defensivas. Los individuos maliciosos que conocen la falta de actualizaciones de seguridad en la infraestructura de una organización pueden explotar dichas debilidades mediante software malicioso que les permita tener acceso a redes. Dichos ataques dirigidos a menudo no son advertidos hasta mucho tiempo después de que hayan ocurrido y de que las repercusiones de dichos ataques se hayan notado.

El término seguridad de red es a menudo malinterpretado como perteneciente exclusivamente a los parches y actualizaciones de seguridad faltantes. Sin embargo la seguridad de red va más allá – hay multitud de vectores de ataque y de debilidades que deben ser tenidas en cuenta. La falta de esfuerzos diligentes y los errores humanos son debilidades de seguridad en sí mismas y pueden ser la causa directa de graves brechas de seguridad. Esto suscita preguntas como: ¿Por qué, a pesar de todas las brechas y amenazas que afligen a las redes, los administradores de sistemas dejan funcionando servicios con las contraseñas predefinidas por los fabricantes? ¿Por qué, a pesar del hecho de que las soluciones anti-malware actualizadas son claves para la protección de toda la red, los profesionales de TI no actualizan las soluciones anti-virus y anti-malware con las últimas firmas? ¿Por qué permiten las empresas el uso sin control de dispositivos portátiles en sus redes? ¿No saben que pueden ser utilizados maliciosamente para coger información empresarial sensible o para traer e

instalar aplicaciones peer-to-peer (P2P) para hacer contrabando de música pirateada, descargar software sin licencia y otros archivos inaceptables en la red? Todo esto lleva a interrupciones en las actividades empresariales diarias y expone a las empresas a amplias responsabilidades legales.

La gestión de vulnerabilidad es el proceso que identifica todas estas cuestiones; un ejercicio de autoevaluación que identifica, clasifica y proporciona la forma de resolver estas debilidades, a la vez que aborda la seguridad desde varios ángulos y vectores de ataque. Es manifiestamente claro que esta es una parte esencial de la seguridad de cualquier red debido a la diligencia del proceso y por lo tanto no coge por sorpresa que el Consejo de Estándares de Seguridad de la Industria de Pagos con Tarjeta profundice en la gestión de vulnerabilidad como parte integral de los requerimientos de cumplimiento PCI DSS.

---

## ¿Cuál es la conexión entre PCI DSS y la gestión de vulnerabilidad?

Mediante PCI DSS, el asunto de seguridad tratado se define tan fuerte como su enlace más débil. La idea general que gobierna PCI DSS aspira a:

- Construir y mantener una red segura
- Proteger la información de titulares de tarjeta en tránsito o inactiva
- Mantener un programa de gestión de vulnerabilidad
- Implementar fuertes medidas de control de acceso
- Monitorizar y probar regularmente su infraestructura de TI
- Mantener una directiva de seguridad de la información.

Para poner alcanzar estos principios, PCI DSS define 12 requerimientos. Los administradores de sistemas tienen que cumplirlos y demostrar sus esfuerzos por cumplirlos. El requerimiento 1 por ejemplo, especifica que deben ser instalados y mantenidos cortafuegos para proteger la información de titulares de tarjeta de ataques externos. Para cumplirlo, los profesionales de TI tienen que escanear sus redes, validar la configuración de los cortafuegos y asegurar que las opciones de configuración no comprometen la seguridad de la red. El requerimiento 6 por otro lado define el desarrollo y mantenimiento de sistemas y aplicaciones seguras – actividad de gestión de vulnerabilidad que supone asegurar que todos los componentes de la red estén actualizados con los últimos parches de seguridad suministrados por los fabricantes.

La gestión de vulnerabilidad sin embargo se extiende a los 12 requerimientos PCI DSS; va más allá de los mecanismos de seguridad de red y alcanza a todos los componentes y entornos de la infraestructura de TI en los que se almacene, procese o transmita información de pagos con tarjeta. Esto incluye:

- Componentes núcleo de la seguridad de red tales como cortafuegos, enrutadores, Sistemas de Prevención de Intrusos (IPS) y Sistemas de Detección de Intrusos (IDS)

- Segmentos de red tales como zonas Desmilitarizadas (DMZ)
- Servidores y sistemas empresariales que albergan servicios DNS, servicios NTP, SMTP/POP3/IMAP y otros servicios de correo, tratamiento de la autenticación, directivas del Directorio Activo, servidores web y servidores de base de datos entre otros
- Aplicaciones internas o web incluyendo software estándar y a medida.

---

## Los problemas de la gestión de vulnerabilidad

Fallar al implementar fuertes métodos de gestión de la vulnerabilidad en todos los componentes listados anteriormente pone a las corporaciones en ruptura con PCI DSS y las expone a amenazas de seguridad internas y externas a la corporación. Las repercusiones de los daños causados por dichas brechas no se limitan sólo a PCI DSS. Las corporaciones pueden tener problemas con leyes y regulaciones locales o nacionales tales como las iniciadas e impuestas por la Comisión Federal de Comercio o sus equivalentes locales. ¡Estas a menudo suponen multas y procedimientos legales por encima de las impuestas por PCI DSS!

A pesar de ser un proceso obligatorio, los profesionales de TI a menudo encuentran la gestión de vulnerabilidad una tarea desalentadora y repetitiva propensa al error humano. Todos los componentes hardware y software de una red corporativa tienen que ser escaneados; la información recogida en un repositorio central, consolidado, comprensible y sobre el que se pueda actuar. Para cumplir esta carga, la automatización es la clave que permite a los profesionales de TI superar desafíos como los siguientes.

**Desafío 1 – Miles de chequeos en todos y cada uno de los equipos:** La célebre [brecha TJX](#) que se hizo pública a principios de este año justifica la gestión de vulnerabilidad. De acuerdo al Vice Presidente y Asociado de Gartner John Pescatore, las debilidades de seguridad de red que expusieron más de 45 millones de registros de tarjetas de crédito y débito podrían haber sido detectadas mediante un escaneo de la vulnerabilidad de la red ([SCMagazine.com](#)). El objetivo del crimen organizado no son sólo las grandes empresas. Hablando en un evento de seguridad en la Casa de los Lores de Londres en Noviembre de 2006, el antiguo consejero de seguridad de la Casa Blanca Howard Schmidt urgía que "las pequeñas y medianas empresas tienen que darse cuenta que sólo porque son pequeñas, no significa que no serán el objetivo. El objetivo de los piratas es cualquier sitio donde pueden conseguir dinero" ([CNET News.com](#)). El 4 de Febrero de 2007, el sitio web de Johnny's Selected Seeds (una relativamente pequeña empresa de 100 empleados de Winslow, Maine, USA) fue pirateado por un intruso y más de 11.500 registros de tarjetas de crédito/débito fueron robados electrónicamente ([MaineToday.com](#)). Aparentemente, la brecha fue observada el 18 de Febrero, cuando dos clientes llamaron a la empresa reclamando que sus tarjetas de crédito habían sido comprometidas con cargos fraudulentos. La automatización de los chequeos de vulnerabilidad de red refuerza la consistencia, reduce el error humano, simplifica la identificación de debilidades de red y le mantiene por delante de las amenazas.

**Desafío 2 – Demasiada información sobre demasiados equipos:** En Marzo de 2007, cerca

de 9 millones de segmentos de registros de información sensible de clientes fueron robados de Dai Nippon Printing Co, por un trabajador subcontratado ([DarkReading.com](http://DarkReading.com)). Esta información, que incluía números de tarjeta de crédito, fueron sacados fuera de la empresa utilizando medios portátiles de almacenamiento. Las rutinas de escaneo tienen que incluir instancia o posición peligrosa fuera de las definiciones de seguridad publicadas. Las modernas soluciones de gestión de vulnerabilidad proporcionan amplias capacidades de auditoría de red que enumeran el hardware y el software no deseable que podría ser potencialmente peligroso para la red – información que por lo tanto no es fácil de conseguir.

**Desafío 3 – La administración de parches es un asunto descuidado:** Con la cantidad de actualizaciones críticas de seguridad liberadas sólo por Microsoft, llegando a la marca de 104 en 2006, ¡los administradores de sistemas tienen buenas razones para sentirse abrumados con la administración de parches! Mediante soluciones automatizadas de administración de parches las corporaciones pueden asegurar que los parches faltantes son descargados automáticamente y puntualmente. No sólo los parches pueden ser implantados/ “empujados” automáticamente en los equipos, también pueden ser retirados para aportar estabilidad a la infraestructura de TI si surge la necesidad.

**Desafío 4 – Las herramientas predefinidas de gestión de vulnerabilidad son limitadas:** Un claro ejemplo es Microsoft Windows Server Update Services (WSUS); una solución que maneja la descarga de actualizaciones Microsoft faltantes sin soporte de ninguna clase para el análisis de vulnerabilidad, la auditoría de red o las operaciones de generación de informes. Esto crea un desafío adicional, que los administradores deben superar – la correlación de resultados. En el caso de otras soluciones especializadas, los administradores también deben dar sentido a los resultados de los análisis de vulnerabilidad, los resultados de auditoría de red y la información de administración de parches mediante la correlación manual de los mismos. Adicionalmente, en la mayoría de los casos, la generación de informes está limitada y por lo tanto el administrador necesitaría gastar más tiempo componiendo manualmente los informes – a menudo mediante operaciones de copiado y pegado.

**Desafío 5 – El cumplimiento de los estándares en un proceso arduo:** La única forma de alcanzar el cumplimiento es mediante informes de amplio alcance que presenten cómo se realiza la gestión de vulnerabilidad y proporcionen pruebas tangibles de cumplimiento. Los problemas aparecen con la cantidad de informes requeridos y con el archivo de tal información. Una vez más, la automatización facilita la vida de los administradores de sistemas mediante la provisión de características que permiten la generación programada de informes y su distribución automática – reforzando los esfuerzos de cumplimiento y ahorrando tiempo, ¡que es tan precioso como el dinero!

Superar todos los desafíos mediante la automatización es una faceta de la solución completa. Otras características, como una base de datos de definición de vulnerabilidades global y bien documentada, así como la capacidad para consolidar diferentes tareas en un único producto también ayudan a los administradores de sistemas a identificar incluso más debilidades

manteniendo por lo tanto la seguridad de la red en perfecto estado. Los administradores de sistemas necesitan herramientas que no sólo automaticen sino que integren también la gestión de vulnerabilidad en sus procesos diarios con los procedimientos menos invasivos posibles; una solución como GFI LANguard Network Security Scanner.

---

## **GFI LANguard Network Security Scanner**

GFI LANguard Network Security Scanner (N.S.S.) es una premiada solución certificada OVAL que detecta, evalúa, informa y rectifica vulnerabilidades presentes en la red. Desde una única solución proporciona análisis de vulnerabilidad y auditoría de redes heterogéneas, capacidades completas de administración de parches así como incomparables características de generación de informes mediante un ReportPack dedicado.

Una versión de GFI LANguard N.S.S. hecha específicamente a la medida del cumplimiento PCI DSS se incluye también en la suite GFI PCI Suite. Esta suite también incluye GFI EventsManager, una solución de administración de registros de sucesos, junto con un paquete de informes hechos a medida. Para más información sobre GFI LANguard N.S.S. y GFI PCI Suite, y como estos productos ayudan a su negocio a alcanzar el cumplimiento PCI DSS visite: <http://www.gfihispana.com/es/pci/>.

---

## **Conclusión**

En la actualidad los profesionales de TI no pueden evadirse de los deberes de la gestión de vulnerabilidad; estos están arraigados en los esfuerzos de diligencia debida y en la obligación del cumplimiento PCI DSS. En el pasado, la supervisión de vulnerabilidades de red era una ardua tarea para cualquier administrador de red. Hoy, soluciones como GFI LANguard N.S.S. presentan características de automatización que ayudan a los profesionales de TI a cumplir con el críticamente importante análisis de vulnerabilidad de red con el menor esfuerzo posible, a la vez que reduciendo costes y la probabilidad del error humano.

---

## Acerca de GFI

GFI es un destacado desarrollador de software que proporciona una única fuente para que los administradores de red dirijan sus necesidades en seguridad de red, seguridad de contenido y mensajería. Con una galardonada tecnología, una agresiva estrategia de precios y un fuerte enfoque en las pequeñas y medianas empresas, GFI es capaz de satisfacer la necesidad de continuidad y productividad de los negocios que tienen las organizaciones en una escala global. Fundada en 1992, GFI tiene oficinas en Malta, Londres, Raleigh, Hong Kong, Adelaide y Hamburgo que soportan más de 200.000 instalaciones en todo el mundo. GFI es una empresa enfocada a canal con más de 10.000 partners en todo el mundo. GFI es también Microsoft Gold Certified Partner. Se puede encontrar más información sobre GFI en <http://www.gfihispana.com>.

© 2007 GFI Software. Todos los derechos reservados. La información contenida en este documento representa la visión del momento de GFI sobre lo discutido a la fecha de la publicación. Como GFI debe responder a las condiciones de los cambios del mercado, no debe ser interpretado como obligación por parte de GFI, y GFI no puede garantizar la exactitud de la información presentada después de la fecha de publicación. Este Documento Blanco solo tiene propósito informativo. GFI NO DA GARANTIA, EXPRESA O IMPLICITAMENTE, EN ESTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor y sus logotipos son marcas registradas o marcas de GFI Software en los Estados Unidos y/o otros países. Todos los nombres de producto o empresas mencionados pueden ser marcas registradas de sus respectivos propietarios.

