

## **PCI DSS sencillo**

### Dirigir el Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta (PCI DSS)

Las principales empresas de tarjetas de crédito están luchando por detener los incidentes de fraude financiero que han afectado a varias organizaciones y a sus consumidores. Consecuentemente, las organizaciones que aceptan transacciones de pagos con tarjeta tienen que comprometerse a cumplir PCI DSS para finales de 2007. Las organizaciones que no puedan cumplir, se arriesgan a no tener permitido el tratamiento de información de titulares de tarjeta y a sanciones de hasta 500.000\$ si los datos son perdidos o robados. Este libro blanco examina los requerimientos necesarios para cumplir con PCI DSS, las implicaciones del no cumplimiento y cómo es de eficaz el papel que juegan la administración de registros de sucesos y la administración de vulnerabilidad de red en la consecución del cumplimiento.

---

## Introducción

Las tarjetas de crédito están muy extendidas y su uso para pagos online se está incrementando drásticamente. Había 1.300 millones de tarjetas de crédito en circulación en USA en 2004, con un 76% de Americanos contando con al menos una tarjeta de crédito. Las ventas de comercio electrónico al detalle en USA en el cuarto de 2006 fueron 33.900\$ millones, un 25% de incremento sobre el mismo trimestre en 2005.

Sin embargo hay malas noticias: El fraude por tarjetas de crédito (25%) fue la forma más común de robo de identidad informada en 2006. Considerando que dicho año las instituciones financieras y empresas perdieron más de 48.000\$ millones debido al robo de identidad, y 5.000\$ millones fueron perdidos por particulares, se puede decir que el fraude por tarjetas de crédito está llegando al fondo de los bolsillos de todos. El fraude del comercio electrónico también está elevándose, alcanzando los 3.000\$ millones en 2006 con un incremento del 7% sobre el 2005. Este documento blanco examina las consecuencias del robo de información de titulares de tarjetas y aborda las siguientes cuestiones clave:

- ¿Qué es la directiva PCI?
- ¿Por qué para su negocio es importante cumplirla?
- ¿Cuáles son las consecuencias de no cumplirla?
- ¿Qué soluciones hay disponibles para abordar la directiva PCI?

---

## Robo y fraude de información de titulares de tarjetas – algunos casos reales

- 18 de Febrero de 2005 – Bank of America acusado de haber perdido más de 1,2 millones de registros de clientes – aunque dijeron que no había evidencia de que la información hubiera caído en manos criminales.
- 16 de Junio de 2005 – CardSystems, proveedor de procesamiento de pagos para comercios, fue demandado en una serie de casos de la acción popular alegando que falló al proteger la información personal de 40 millones de clientes. El negocio de CardSystems encaraba el colapso ya que VISA y American Express cortaron sus lazos con la empresa, prohibiéndola procesar información de sus tarjetas. CardSystems fue posteriormente adquirida por otra empresa.
- 9 de Febrero de 2006 – Se estimó que alrededor de 200.000 cuentas de tarjetas de débito fueron reveladas por comercios al detalle desconocidos, aparentemente OfficeMax y otros. Estas incluían cuentas relacionadas con comerciantes de bancos y sociedades de crédito a escala nacional tales como CitiBank y Wells Fargo.

- 31 de Enero de 2006 – Boston Globe y The Worcester Telegram & Gazette expusieron involuntariamente 240.000 registros de tarjetas de crédito y débito, junto con información de ruta de cheques personales, impresos en papel usado reciclado para envoltorios para la distribución de periódicos.
- 12 de Enero de 2007 – MoneyGram, un proveedor de medio de pago, informó que un servidor de la empresa fue ilegalmente accedido desde Internet el mes pasado. Contenía información de unos 79.000 recibos de pago de clientes, incluyendo nombres, direcciones, números de teléfono y, en algunos casos, números de cuenta bancaria.
- 17 de Enero de 2007 – TJX Companies Inc. anunció públicamente que había experimentado una intrusión no autorizada en el sistema electrónico de procesamiento de información de tarjetas de crédito/débito. En la que es considerada como la más fascinante brecha de seguridad hasta la fecha, hasta 45.700.000 números de cuenta de tarjetas de crédito/débito y más de 455.000 registros de devolución de mercancía (conteniendo nombres y números de permiso de conducción de clientes) fueron robados del sistema de TI de la empresa.

Los grandes detallistas online no son las únicas organizaciones en el punto de mira. La atención pública puede estar fijada en las grandes pérdidas de información, pero los expertos en fraude financiero dicen que los hackers están fijando el objetivo cada vez más en pequeños sitios web comerciales. En algunos casos, los criminales son capaces de conseguir acceso en tiempo real a la información de las transacciones de sitios web, permitiéndoles robar números válidos de tarjeta de crédito y rápidamente realizar gran número de compras fraudulentas. Los pequeños negocios electrónicos ofrecen menos víctimas, pero a menudo suponen un objetivo más sencillo, debido a defectos en las aplicaciones utilizadas para procesar pedidos o por una sobre confianza en la subcontratada seguridad del sitio.

El ciber crimen y la amenaza que acompaña al robo de identidad reducen la confianza del usuario y consumidor, ralentizando la aceptación del comercio electrónico. Como resultado, la seguridad informática, actividad crítica que ayuda a proteger estos sistemas, ha pasado a una posición de importancia.

---

## **Directiva de la Industria de Pagos con Tarjeta (PCI)**

El marco de seguridad de datos de la Industria de Pagos con Tarjeta (PCI) fue creado por American Express, Discover Financial Services, JCB, MasterCard Worldwide, y Visa Internacional. Antes de 2004, cada una de las asociaciones tenía un conjunto propietario de requerimientos de seguridad de la información que a menudo eran agobiantes y repetitivas para los participantes en redes de varias marcas. Posteriormente las asociaciones crearon un conjunto uniforme de requerimientos de seguridad de la información para todas las marcas nacionales de tarjetas (exclusiva de boutiques y etiquetas privadas). Estos requerimientos han

pasado a ser conocidos como el Estándar de Seguridad de Datos PCI (PCI DSS), que rige en todos los canales de pago: Venta al detalle, por correo, por teléfono y comercio electrónico.

## El marco PCI DSS

El marco PCI DSS está dividido en 12 requerimientos de seguridad (VISA se refiere a ellos como la 'Docena Digital') que están organizados en las siguientes seis categorías:

PCI DSS
<b>Crear y mantener una red segura</b>
Requerimiento 1: Instalar y mantener un cortafuegos para proteger la información de titulares de tarjetas Requerimiento 2: No utilizar las contraseñas ni otros parámetros de seguridad predefinidos por el fabricante del sistema
<b>Proteger la información de los titulares de tarjetas</b>
Requerimiento 3: Proteger la información almacenada de titulares de tarjetas Requerimiento 4: Encriptar la transmisión de información de titulares de tarjetas a través de redes abiertas, públicas.
<b>Mantener un programa de administración de vulnerabilidad</b>
Requerimiento 5: Utilizar y actualizar regularmente el software o las aplicaciones anti-virus Requerimiento 6: Desarrollar y mantener sistemas y aplicaciones seguros
<b>Implementar fuertes medidas de control de acceso</b>
Requerimiento 7: Restringir el acceso a la información de titulares de tarjetas según la necesidad-de-saber Requerimiento 8: Asignar un ID único a cada persona con acceso a ordenadores Requerimiento 9: Restringir el acceso físico a la información de titulares de tarjetas
<b>Monitorizar y testear regularmente las redes</b>
Requerimiento 10: Rastrear y monitorizar todo acceso a los recursos de red y a la información de titulares de tarjetas Requerimiento 11: Testear regularmente la seguridad de los sistemas y procesos
<b>Mantener una directiva de seguridad de la información</b>
Requerimiento 12: Mantener una directiva que dirija la seguridad de la información para empleados y contratistas

**Tabla 1: El marco PCI DSS**

El cumplimiento de estos requerimientos se puede resumir en 3 etapas principales:

- **Recogida y almacenamiento:** Recogida segura y almacenamiento inalterable de todos los datos de registros de forma que estén disponibles para análisis.
- **Generación de informes:** Ser capaz, en caso de auditoría, de probar en el acto el cumplimiento y presentar evidencias de que existen los controles para la protección de

datos.

- **Monitorización y alarma:** Tener sistemas tales como el auto-aviso, para ayudar a los administradores a monitorizar constantemente el acceso y uso de información. Los administradores son inmediatamente avisados de problemas y pueden tratarlos rápidamente. Estos sistemas también deben extenderse a los mismos datos de registro – debe probarse que los datos de registros son recogidos y almacenados.

### **Niveles de comercios y proveedores de servicio**

Los comercios y los proveedores de servicios que deben cumplir con PCI DSS están clasificados de acuerdo al número de transacciones con tarjeta que procesan en un período de 12 meses. Las siguientes tablas 2 y 3 describen los varios niveles y requerimientos de cumplimiento para ambos comercios y proveedores de servicios.

Los **Comercios** son aceptadores autorizados de tarjetas para el pago de bienes y servicios. Ejemplos de industrias en las que los comercios deben cumplir incluyen, pero no están limitadas a:

- Comercio online como el detallista online Amazon.com
- Al detalle como los comercios al detalle Wal-Mart
- Educación superior como universidades
- Salud como hospitales
- Viajes y entretenimiento como hoteles y restaurantes
- Energía como gasolineras
- Finanzas como bancos y compañías aseguradoras

NIVELES DE COMERCIOS	
DEFINICION DE COMERCIO	CUMPLIMIENTO
<b>Nivel 1</b>	
<ul style="list-style-type: none"> <li>Comercios cuya información de titulares de tarjetas ha estado comprometida</li> <li>Comercios con más de seis millones de transacciones con tarjeta de crédito anualmente a través de todos los canales, incluyendo comercio electrónico</li> </ul>	<ul style="list-style-type: none"> <li>Valoración anual in-situ de la seguridad de información PCI y escaneos de red trimestrales</li> </ul>
<b>Nivel 2</b>	
<ul style="list-style-type: none"> <li>Comercios con entre 1 y 6 millones de transacciones con tarjeta de crédito anualmente</li> </ul>	<ul style="list-style-type: none"> <li>Auto valoración anual y escaneos de red trimestrales</li> </ul>
<b>Nivel 3</b>	
<ul style="list-style-type: none"> <li>Comercios con entre 20.000 y 1.000.000 de transacciones con tarjeta de crédito anualmente</li> </ul>	<ul style="list-style-type: none"> <li>Auto valoración anual y escaneos de red trimestrales</li> </ul>
<b>Nivel 4 **</b>	
<ul style="list-style-type: none"> <li>Todo el resto de comercios</li> </ul>	<ul style="list-style-type: none"> <li>Auto valoración anual y escaneos de red trimestrales</li> </ul>

**Tabla 2: Niveles de comercios**

\* Los niveles de comercios se basan en definiciones de Visa USA

\*\* La PCI DSS requiere que todos los comercios realicen escaneos externos de red para conseguir el cumplimiento. Los receptores pueden requerir la emisión de informes de escaneos y/o cuestionarios de los comercios de nivel 4.

Los **Proveedores de Servicios** son organizaciones que procesan, almacenan o transmiten información de titulares de tarjetas en nombre de miembros, comercios u otros proveedores de servicios. Ejemplos de proveedores de servicios que deben cumplir incluyen, pero no están limitados a:

- Pasarelas de pago
- Proveedores de alojamiento de comercio electrónico
- Proveedores de servicios gestionados
- Agencias de informes de crédito
- Empresas de gestión de copias de seguridad
- Empresas de destrucción de papel

DEFINICION DE PROVEEDOR DE SERVICIOS	CUMPLIMIENTO
<b>Nivel 1</b>	
Todos los procesadores (miembros y no miembros) y todas las pasarelas de pago.*	Valoración anual in-situ de la Seguridad de Información PCI y escaneos de red trimestrales
<b>Nivel 2</b>	
Cualquier proveedor de servicios que no está en el Nivel 1 y almacena, procesa o transmite más de 1 millón de cuentas/transacciones de tarjeta de crédito anualmente	Valoración anual in-situ de la Seguridad de Información PCI y escaneos de red trimestrales
<b>Nivel 3</b>	
Cualquier proveedor de servicios que no está en el Nivel 1 y almacena, procesa o transmite menos de 1 millón de cuentas/transacciones de tarjeta de crédito anualmente	Cuestionario de auto valoración anual y escaneos de red trimestrales

**Tabla 3: Niveles de proveedor de servicios**

\* Las pasarelas de pago son una categoría de agente o proveedor de servicios que almacena, procesa y/o transmite información de titulares de tarjeta como parte de una transacción de pago (por ejemplo, PayPal). Específicamente, permiten transacciones de pago (por ejemplo, autorización o acuerdo) entre comercios y procesadores (por ejemplo, puntos finales VisaNet). Los comercios pueden enviar sus transacciones de pago directamente a un punto final, o indirectamente a una pasarela de pagos.

#### Rigurosos límites de cumplimiento

Las principales empresas de tarjetas están presionando duramente a los comerciantes que deben acatar el cumplimiento de PCI DSS. Se han situado varios límites de tiempo y fijado fuertes sanciones y multas para las organizaciones que fallen en llegar a tiempo a la línea de meta. Entre importantes fechas límite, Visa USA ha fijado:

- 31 de Marzo de 2007 – La fecha límite por la que los comerciantes de nivel 1 y 2 deben

demostrar que no están almacenando datos de seguimiento completos, CVV2 o PIN.

- 30 de Septiembre de 2007 – Fecha para la cual se espera que todos los comerciantes de nivel 1 estén cumpliendo completamente PCI DSS.
- 31 de Diciembre de 2007 – Fecha para la cual se espera que todos los comerciantes de nivel 2 estén cumpliendo completamente PCI DSS.

Las fechas límite para el cumplimiento pueden variar entre asociaciones de tarjetas y regiones; por lo tanto los comerciantes y proveedores de servicios indecisos deben tomar la decisión de consultar a adquirentes o asociaciones de tarjetas para sus respectivas fechas límite.

---

## ¿Por qué para su negocio es importante cumplirla?

Aunque es un estándar liderado por USA, PCI DSS es un requerimiento global para todas las entidades que manejan información de titulares de tarjeta. No todos los países son conscientes de esto, por ejemplo, la generalizada confusión en la industria bancaria de Australia sobre las nuevas medidas de cumplimiento ha llevado a cinco brechas de la PCI DSS durante 2006.

Está en el propio interés de los bancos adquirentes asegurar que sus comercios son conscientes y cumplen con PCI DSS. La razón es bastante lógica – los bancos adquirentes son los actores principales que crean la línea de confianza entre las empresas de tarjetas y los comercios – consecuentemente son también los que están directamente en la línea de fuego frente a las empresas de tarjetas de crédito/débito cuando uno o más de sus comercios sufren una brecha. Para mantener una satisfactoria y saludable relación comercial con las empresas de tarjetas, los bancos adquirentes deben asegurar que sus comercios están protegidos adecuadamente, y que PCI DSS es la herramienta que calibra la seguridad de la información de titulares de tarjetas por parte del comercio.

Similarmente, los comercios y proveedores de servicios están esperando demostrar su nivel de cumplimiento con PCI DSS. Esto ayuda a mantener una saludable relación comercial con los bancos adquirentes y a evitar responsabilidades por no cumplimiento.

---

## ¿Cuáles son las consecuencias de no cumplirla?

Las empresas de tarjetas pueden imponer multas a sus instituciones bancarias miembros cuando se descubre que los comercios no cumplen con PCI DSS. Los bancos adquirentes pueden a su vez obligar contractualmente a los comercios a indemnizarlos y compensarlos por dichas multas. Las multas podrían llegar a 500.000\$ por incidencia si la información está comprometida y se descubre que los comercios no satisfacen el cumplimiento. En el peor escenario, los comercios también podrían arriesgarse a perder la capacidad de procesar transacciones de tarjetas de crédito de clientes.

Los negocios cuya información de titulares de tarjeta haya estado comprometida están

obligados a notificarlo a las autoridades legales y se espera que ofrezcan servicios gratuitos de protección de crédito a aquellos potencialmente afectados.

Podría haber otras consecuencias además de las sanciones. La pérdida de datos de titulares de tarjetas, ya sea accidental o por robo, también puede llevar a la toma de acciones legales por los titulares de las tarjetas. Dicho paso supondrá mala publicidad, que puede a su vez llevar a la pérdida de negocio.

---

## **¿Qué soluciones proporciona GFI para ayudarle a cumplir los requerimientos PCI?**

Se pueden implantar soluciones tecnológicas para automatizar algunas de las tareas que necesita abordar para satisfacer los requerimientos PCI. Estas soluciones le permiten monitorizar la adhesión al estándar y le avisan cuando tienen lugar sucesos no autorizados relativos a información de titulares de tarjetas. GFI proporciona herramientas software que le ayudan a hacer exactamente esto.

GFI EventsManager, GFI LANguard Network Security Scanner (N.S.S.) y GFI EndPointSecurity son tres galardonados productos de seguridad de red de GFI. Mediante la auditoría, monitorización, generación de informes y alerta estos productos pueden ayudarle a dirigir varias secciones de nueve de los 12 requerimientos PCI, como se ilustra en la Tabla 4 siguiente.

REQUERIMIENTOS PCI DSS			
	GFI EventsManager	GFI LANguard N.S.S.	GFI EndPointSecurity
1. Instalar y mantener un cortafuegos para proteger la información de titulares de tarjetas	•	•	
2. No utilizar las contraseñas ni otros parámetros de seguridad predefinidos por el fabricante del sistema	•	•	
3. Proteger la información almacenada de titulares de tarjetas	•		•
4. Encriptar la transmisión de información de titulares de tarjetas a través de redes abiertas, públicas.			
5. Utilizar regularmente software o aplicaciones anti-virus actualizados		•	
6. Desarrollar y mantener sistemas y aplicaciones seguros		•	
7. Restringir el acceso a la información de titulares de tarjetas según la necesidad-de-saber	•		
8. Asignar un ID único a cada persona con acceso a ordenadores	•	•	
9. Restringir el acceso físico a la información de titulares de tarjetas			
10. Rastrear y monitorizar todo acceso a los recursos de red y a la información de titulares de tarjetas	•	•	
11. Testear regularmente la seguridad de los sistemas y procesos	•	•	•
12. Mantener una directiva que dirija la seguridad de la información para empleados y contratistas			

Tabla 4: Requerimientos PCI DSS

## **GFI EventsManager**

El análisis de la información de sucesos está directamente especificada en el requerimiento 10 (Tabla 4) pero monitorizar los sucesos es una buena práctica para cualquier organización.

En un entorno de red típico, la información de sucesos está distribuida y es voluminosa y críptica. Las herramientas de análisis de sucesos suministradas junto con la mayoría de sistemas operativos ofrecen sólo las más básicas características. Como resultado, los administradores no tienen forma de ser avisados cuando se registrar sucesos concretos importantes o problemáticos, tales como el acceso no autorizado a información de titulares de tarjetas. Las utilidades de examen y filtrado de sucesos proporcionadas por estas herramientas tienen muy limitadas capacidades de búsqueda y filtrado.

GFI EventsManager es una completa solución de administración de registros que vence todos estos obstáculos, permitiéndole centralizar los sucesos, automatizar la recogida de sucesos, recibir alertas y emitir informes de investigación. Cuando se recogen sucesos, los conjuntos de reglas incluidos en GFI EventsManager procesan los sucesos para clasificarlos y activar alertas/acciones en consecuencia. Uno de los conjuntos predefinidos proporcionado está específicamente orientado hacia la clasificación de los sucesos en base a los requerimientos PCI. El análisis de sucesos puede llevarse a cabo mediante el examinador de sucesos incluido; también se pueden crear y ejecutar consultas para recuperar y analizar sucesos concretos.

Mediante GFI EventsManager los negocios pueden asegurar que todos los sucesos relacionados con la información de titulares de tarjetas están siendo constantemente monitorizados. Para más información y descargar el producto, visite <http://www.gfihispana.com/es/eventsmanager/>.

## **GFI LANguard Network Security Scanner**

La administración de vulnerabilidad es central para los requerimientos 5 y 6 (Tabla 4). Sin embargo, ser capaz de detectar vulnerabilidades en varias áreas cubiertas por otros requerimientos es de extrema importancia.

GFI LANguard Network Security Scanner (N.S.S.) dirige los tres pilares de la administración de vulnerabilidad: análisis de seguridad, administración de parches y auditoría de red en una solución integrada. GFI LANguard N.S.S. escanea toda la red buscando más de 15.000 vulnerabilidades, identifica todos los posibles problemas de seguridad y proporciona a los administradores las herramientas que necesitan para detectar, evaluar, informar y remediar cualquier amenaza antes de que lo hagan los hackers.

Manejar separadamente problemas relacionados con la vulnerabilidad, la administración de parches y la auditoría de red, a veces utilizando varios productos, es una importante preocupación para los administradores. No solo tienen que instalar, aprender a manejar y administrar varias soluciones, sino que gastan la mayor parte de su tiempo intentando

comprender dónde están los problemas en lugar de tratar realmente las amenazas que puedan estar presentes. Utilizando una única consola con amplias funcionalidades de generación de informes, la solución integrada GFI LANguard N.S.S. ayuda a los administradores a dirigir estos asuntos más rápida y eficazmente.

Mediante GFI LANguard N.S.S. los negocios pueden asegurar que la información de titulares de tarjetas se mantiene en un entorno seguro. Para más información y descargar el producto, visite <http://www.gfihispana.com/es/lannetscan/>.

### **GFI EndPointSecurity**

Proteger la información almacenada de titulares de tarjetas, requerimiento 3 (Tabla 4), es un requerimiento clave del estándar de seguridad de datos PCI. Asegurar que estos datos no caen en malas manos es crucial.

Es un hecho bien conocido que los dispositivos de almacenamiento masivo, tales como las unidades USB, han crecido en popularidad en los últimos años. Son sencillos y fáciles de instalar, capaces de almacenar enormes cantidades de información, y suficientemente pequeños para llevarlos en un bolsillo. Sin mecanismos de seguridad, copiar toda la información de titulares de tarjetas en dichos dispositivos puede ser fácil y rápidamente realizado.

GFI EndPointSecurity es la solución de seguridad que le ayuda a mantener la integridad de la información evitando la transferencia no autorizada de contenido a y desde los dispositivos portátiles de almacenamiento. Mediante su tecnología, GFI EndPointSecurity le habilita para permitir o denegar el acceso a un dispositivo así como asignar (donde sea aplicable) privilegios 'control total' o 'sólo lectura' sobre un dispositivo particular o a un usuario/grupo local o del Directorio Activo. Con GFI EndPointSecurity puede registrar la actividad de todos los dispositivos portátiles que estén siendo utilizados en sus equipos de red, incluyendo la fecha/hora de uso y por quien fue utilizado el dispositivo.

Mediante GFI EndPointSecurity los negocios pueden asegurar que la información de titulares de tarjetas no está siendo copiada en dispositivos de almacenamiento no autorizados. Para más información y descargar el producto, visite <http://www.gfihispana.com/es/endpointsecurity/>.

### **GFI ReportCenter**

GFI ReportCenter es un marco centralizado de informes que le permite la generación de varios informes utilizando datos recogidos por cada uno de los productos GFI. GFI EventsManager, GFI LANguard N.S.S. y GFI EndPointSecurity tienen todos ReportPacks que se integran en el marco GFI ReportCenter.

Estos ReportPacks son potentes complementos de generación de informes con numerosos informes preconfigurados. Además incluyen un conjunto integral de características tales como programación de informes, exportación de informes y distribución automática de informes por

correo electrónico. Los informes generados mediante los ReportPacks son valiosos para los negocios cuando se valora la efectividad en el cumplimiento del programa PCI. Para más información y descargar un ReportPack, visite <http://www.gfihispana.com/es/reportcenter/>.

### **Incentivos**

Es del interés de las organizaciones mantener la información de tarjetas de crédito de forma que cumpla con el Estándar de Seguridad de Datos PCI. También es del interés de los bancos asegurar que los comercios cumplen.

Los bancos podrían ofrecer incentivos a los comercios para cumplir la directiva ofreciéndoles licencias de los productos de seguridad de red GFI como parte de la firma de los acuerdos. Además podrían proporcionar servicios adicionales, tales como experiencia técnica en los productos GFI. Esta sería una situación ganador-ganador ya que los comercios pueden tener la seguridad de cumplir con PCI DSS, a la vez que tienen todo el resto de beneficios proporcionados por los productos GFI. Los bancos también puede tener la seguridad de saber que los comercios a los que han autorizado a aceptar pagos con tarjeta de crédito han dado un gran paso adelante para conseguir el cumplimiento.

---

### **Conclusión**

Las empresas están en riesgo constante de pérdida de información sensible sobre titulares de tarjetas. Dicha pérdida supondrá sanciones, acciones legales y mala publicidad. Esto llevará a su vez a pérdida de negocio. Conseguir el cumplimiento del Estándar de Seguridad de Datos PCI debe ser una prioridad en la agenda de las organizaciones que llevan a cabo transacciones empresariales que implican el uso de tarjetas de crédito.

Implementar herramientas software para la administración de registros, la gestión de vulnerabilidad, el análisis de seguridad y la seguridad de punto final le ayudará a dar un gran paso para conseguir el cumplimiento. Los productos de seguridad de red de GFI le pueden ayudar precisamente a esto.

---

## 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>.



---

## Fuentes

CreditCards.com (2006) *Credit Card Industry Facts and Personal Debt Statistics* disponible en: <http://www.creditcards.com/statistics/statistics.php> (última cita 29 Dec 2006).

U.S. Census Bureau (2006) *Quarterly retail e-commerce sales 2nd quarter 2006* disponible en: <http://www.census.gov/mrts/www/data/html/06Q2.html> (última cita 29 Dic 2006).

Federal Trade Commission (2006) *Consumer Fraud and Identity Theft Complaint Data January – Diciembre 2005*.

United States Postal Service *Identity Theft: Stealing Your Name and Your Money* disponible en: <http://www.usps.com/postalinspectors/IDtheft2.htm> (última cita 29 Dic 2006).

Bednarz A. (2006) *Online merchants will lose \$3 billion to fraud in 2006*, Network World, Inc. disponible en: <http://www.networkworld.com/news/2006/111406-online-merchants-fraud.html?nlhtsec=1113securityalert2> (última cita 29 Dic 2006).

Marlin S. (2005) *Customer Data Losses Blamed On Merchants And Software*, CMP Media LLC disponible en: <http://www.informationweek.com/showArticle.jhtml?articleID=161601930> (última cita 29 Dic 2006).

Ward M. (2005) *Web shops face tighter security*, BBC disponible en: <http://news.bbc.co.uk/2/hi/technology/4449759.stm> (última cita 29 Dec 2006).

Evers J. (2005) *Credit card breach exposes 40 million accounts*, CNET Networks, Inc. disponible en: [http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029\\_3-5751886.html](http://news.com.com/Credit+card+breach+exposes+40+million+accounts/2100-1029_3-5751886.html) (última cita 29 Dic 2006).

Extended Retail Solutions (2006) *Fighting spyware and retail identity theft*, GDS Publishing Ltd. disponible en: <http://www.extendedretail.com/pastissue/article.asp?art=25770&issue=147> (última cita 29 Dic 2006).

Schneier B. (2005) *Schneier on Security: Visa and Amex Drop CardSystems*, Schneier.com disponible en: [http://www.schneier.com/blog/archives/2005/07/visa\\_and\\_amex\\_d.html](http://www.schneier.com/blog/archives/2005/07/visa_and_amex_d.html) (última cita 29 Dic 2006).

Harris Interactive (2005) *Global Consumer Attitudes and Behaviors Toward Data Security*, Visa International.

Krebs B. (2006) *ID Thieves Turn Sights on Smaller E-Businesses*, The Washington Post disponible en: <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800333.html> (última cita 29 Dic 2006).

Cybertrust (2006) *PCI Merchant & Service Provider Levels* disponible en:

[http://www.cybertrust.com/solutions/compliance\\_governance/pci\\_compliance/pci\\_levels/](http://www.cybertrust.com/solutions/compliance_governance/pci_compliance/pci_levels/) (última cita 29 Dic 2006).

MasterCard *Merchant Levels Defined* disponible en: [http://www.mastercard.com/us/sdp/merchants/merchant\\_levels.html](http://www.mastercard.com/us/sdp/merchants/merchant_levels.html) (última cita 29 Dic 2006).

Pauli D. (2006) *Australian Compliance Confusion Leads to Security Breaches*, CXO Media Inc. disponible en: [http://www2.csoonline.com/blog\\_view.html?CID=25049](http://www2.csoonline.com/blog_view.html?CID=25049) (última cita 29 Dic 2006).

Wells Fargo *Merchant Services - Payment Card Industry (PCI) Data Security Standards FAQs* disponible en: <https://www.wellsfargo.com/biz/help/merchant/faqs/pci#Q24> (última cita 29 Dic 2006).

PCI Security Standards Council (2006) *Payment Card Industry (PCI) Data Security Standard* (Version 1.1) disponible en: [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf).

© 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.