



# Salvaguardando los Datos de las Cuentas de los Tarjetahabientes

## Cómo Facilita el Software Reflection el Cumplimiento con PCI

### CONTENIDO

Los Doce Requerimientos PCI .....	1
Cómo Maneja Reflection Tus Dificultades de Seguridad Relacionadas con Hosts .....	2
La Ruta de Reflection al Cumplimiento .....	3
Más Capacidades, Cumplimiento Más Rápido .....	5

# Salvaguardando los Datos de las Cuentas de los Tarjetahabientes

## Cómo Facilita el Software Reflection el Cumplimiento con PCI

En 2004, las principales compañías de tarjeta de crédito—incluyendo a Visa, MasterCard, y American Express—unieron fuerzas para crear el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). El PCI DSS aplica a todas las compañías que almacenen, procesen o transmitan datos de cuenta de tarjetahabientes. Su propósito: garantizar la privacidad de la información para los consumidores por medio de estrictos controles de seguridad en toda la industria.

Una serie de fechas límite para el cumplimiento han confundido a las organizaciones respecto al cumplimiento de los 12 extensos requerimientos PCI DSS. Estos requerimientos van desde cosas relativamente fáciles de implementar—como asegurarse de mantener actualizado el software antivirus—hasta cosas complejas y demandantes—como rastrear el acceso a los recursos de red y a la información de los tarjetahabientes.

Este informe técnico le detalla cómo los emuladores de terminal, las utilerías para la transferencia de archivos así como los clientes y servidores SSH de Attachmate® Reflection® pueden ayudarle a lograr el cumplimiento con PCI DSS. Para cuando acabe la lectura, usted sabrá qué productos Reflection pueden ayudarle a afrontar requerimientos PCI específicos—y como lo hacen. También verá que Reflection permite el cumplimiento más allá de la emulación de terminal y la transferencia de archivos, adentrándose en áreas que usted puede que no haya considerado antes.

### Los Doce Requerimientos PCI

El PCI DSS consiste de doce requerimientos diseñados para ayudar a garantizar que la información del tarjetahabiente esté segura, y que la red y sistemas que manejan los datos estén bien protegidos. Los doce requerimientos entran en estos grupos:

<p><b>Desarrollar y Mantener una Red Segura</b></p> <ol style="list-style-type: none"> <li>1. Instalar y mantener una configuración de firewall para proteger los datos.</li> <li>2. No usar las contraseñas del sistema y ni otros parámetros de seguridad suministrados por default por los vendedores de software.</li> </ol>
<p><b>Proteger los Datos del Tarjetahabiente</b></p> <ol style="list-style-type: none"> <li>3. Proteger los datos almacenados.</li> <li>4. Encriptar los datos del tarjetahabiente e información confidencial transmitida a través de redes públicas.</li> </ol>
<p><b>Mantener un Programa de Manejo de Vulnerabilidad</b></p> <ol style="list-style-type: none"> <li>5. Usar y actualizar regularmente el software antivirus.</li> <li>6. Desarrollar y mantener sistemas y aplicaciones seguras.</li> </ol>
<p><b>Implementar Medidas Sólidas de Control de Acceso</b></p> <ol style="list-style-type: none"> <li>7. Restringir el acceso a los datos tomando como base la necesidad de conocer la información.</li> <li>8. Asignar una Identificación única a cada persona que tenga acceso a una computadora.</li> <li>9. Restringir el acceso físico a los datos de los tarjetahabientes.</li> </ol>
<p><b>Monitorear y Probar Regularmente las Redes</b></p> <ol style="list-style-type: none"> <li>10. Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabiente.</li> <li>11. Probar regularmente los sistemas y procesos de seguridad.</li> </ol>
<p><b>Mantener una Política de Seguridad de la Información</b></p> <ol style="list-style-type: none"> <li>12. Mantener una política que contemple la seguridad de la información.</li> </ol>

Los productos Reflection facilitan el cumplimiento con los requerimientos 1, 2, 4, 6, 7, 8, y 10.

## Cómo Maneja Reflection Tus Dificultades de Seguridad Relacionadas con Hosts

Para ayudarte a entender como los productos Reflection pueden facilitar el cumplimiento con PCI, esta sección resume problemas clave de seguridad relacionados con los hosts y describe cómo los productos Reflection los afrontan.

### Seguridad para Servidores

Los sistemas Host almacenan la información de los tarjetahabientes y corren aplicaciones que permiten el acceso a esos datos. Los sistemas Host también pueden ser servidores de archivos que mantienen información de tarjetahabientes en archivos que necesitan ser transferidos sobre redes públicas. Debido a la naturaleza confidencial de esta información, las organizaciones necesitan restringir el acceso a estos datos y encriptarlos cuando viajan sobre una red.

**Solución Reflection:** Reflection for Secure IT es una familia de clientes y servidores Secure Shell para Windows® y UNIX. Con los servidores Reflection for Secure IT, usted puede crear túneles seguros y encriptados para datos en movimiento—incluyendo comunicaciones desde los emuladores basados en cliente, utilerías de transferencia de archivos o cualquier otra aplicación que utilice el protocolo TCP/IP.

Reflection for Secure IT también realiza otra función crítica de seguridad—registra los accesos, incluyendo los accesos con privilegios de administrador, a los componentes del sistema. Al permitir la configuración de registros de auditoría, Reflection for Secure IT ofrece información clave (quién y cuándo accedió al sistema por medio del servidor SSH) a los medios estándar de registro en el sistema host.

### Seguridad para Workstations

Los usuarios y administradores de sistemas frecuentemente se respaldan en utilerías basadas en cliente para el acceso a archivos y aplicaciones host. Tanto las contraseñas y la identificación de usuario utilizados para ganar acceso a los sistemas host, como la información confidencial que pasa entre la estación de trabajo y el sistema host, todo ello necesita estar protegido de las miradas curiosas mientras está en tránsito.

**Solución Reflection:** Los emuladores de terminal Reflection for Windows y Reflection for the Web soportan una gran variedad de tecnologías de encriptación (incluyendo SSH y SSL/TLS) y métodos de autenticación (como Kerberos) que igualan las capacidades habilitadas en el sistema host. Con este soporte, los jefes de seguridad pueden sentirse seguros de que tanto las credenciales de las cuentas de los usuarios (como son las contraseñas) y la información confidencial (como puede ser la información de

## Acerca de los productos Reflection

### Reflection for Windows

Los productos Reflection de emulación de terminal (así como también los emuladores de terminal Attachmate EXTRA!® e INFOConnect®) hacen conexiones seguras a aplicaciones sobre sistemas IBM, HP, UNIX, Unisys, OpenVMS, Tandem, CRS/GDS. Estos productos, ricos en características y de probada calidad, proporcionan un conjunto completo de opciones de encriptación, autenticación e integridad de datos.

### Reflection Secure FTP

Incluido con los productos Reflection, EXTRA! e INFOConnect, Reflection Secure FTP proporciona una utilería robusta para la transferencia de archivos entre las estaciones de trabajo de los usuarios y los sistemas host.

### Reflection for the Web

Reflection for the Web es un software de emulación de terminal que conecta de forma segura los navegadores web de los usuarios a aplicaciones IBM, HP, UNIX, Linux, OpenVMS, Unisys, y CRS/GDS. Con sus fuertes capacidades de autenticación y autorización de usuarios, registros de auditoría, encriptación y control de acceso, puede ofrecer de forma segura aplicaciones host completamente funcionales a través de Internet.

### Reflection for Secure IT

Reflection for Secure IT es una familia de clientes y servidores Secure Shell para los entornos Windows y UNIX—todos diseñados para proteger datos en movimiento. Con las capacidades de encriptación, autenticación, auditoría e integridad de datos de Reflection for Secure IT, usted puede transferir datos confidenciales, manejar servidores remotos y acceder a aplicaciones corporativas por medio de conexiones encriptadas.

tarjetahabientes) será encriptada mientras pasan entre el host y la pantalla de emulación de terminal.

Los clientes Reflection Secure FTP, incluidos con los productos de emulación Reflection, también soportan una diversa variedad de tecnologías y métodos de encriptación. Estas tecnologías y métodos ayudan a garantizar que los archivos que contienen información confidencial no puedan ser accedidos por usuarios no autorizados, porque son encriptados antes de que entren en la red.

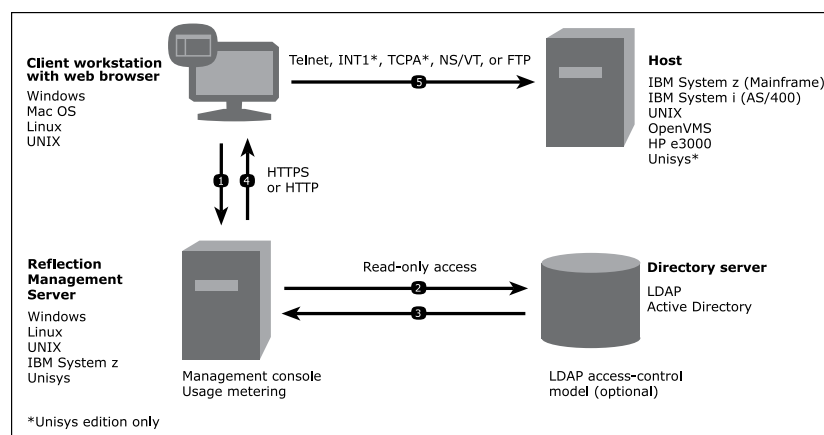
### Seguridad para el Sistema de Acceso

Los clientes de emulación de terminal proporcionan acceso a datos privados en el host—lo cual significa que

las sesiones de emulación deben estar estrechamente controladas.

**Solución Reflection:** Reflection for the Web proporciona autenticación y control de acceso que aprovecha los directorios existentes de usuario (como Active Directory). Los usuarios no pueden acceder a las sesiones de emulación a menos que hayan sido aprobados por un administrador.

Se pueden asignar configuraciones específicas de sesión a los usuarios y grupos dentro de un dominio. Estas sesiones son ejecutadas por medio de enlaces en una página web o portal protegido. Cuando los usuarios acceden a la página, son autenticados contra el directorio de usuarios y se les permite el acceso solo a sesiones host pre-asignadas.



- 1) El usuario se conecta al Reflection Management Server.
- 2) El usuario se autentica ante un servidor de directorio (LDAP/Active Directory)-opcional.
- 3) El servidor de directorio proporciona identificación de usuario y grupo.
- 4) Reflection Management Server envía la sesión de emulación para autenticar al cliente.
- 5) El usuario autenticado se conecta al host.

## La Ruta de Reflection al Cumplimiento

Esta sección explica cómo puede ayudarle Reflection a cumplir con los requerimientos 1, 2, 4, 6, 7, 8, y 10 del PCI DSS.

### Requerimiento 1: Instalar y mantener una configuración de firewall para proteger los datos

La Sección 1.1 de la documentación del PCI DSS especifica que ciertos protocolos—incluyendo Secure Sockets Layer (SSL) y Secure Shell (SSH)—pueden pasar a través del firewall sin documentación o justificación especial. Pero protocolos como el FTP, que son considerados de riesgo, requieren de documentación y justificación para permitir que pasen a través del firewall.

La Sección 1.2 especifica que los firewalls deben estar configurados para denegar todo el tráfico—excepto para los protocolos requeridos por el entorno de datos de los tarjetahabientes—de redes no confiables.

A continuación cómo los productos Reflection facilitan el cumplimiento con el Requerimiento 1:

### Reflection for Windows

Todos los productos Reflection for Windows soportan la encriptación del flujo de datos de la terminal por medio de protocolos aceptables de seguridad, incluyendo SSH y SSL/TLS.

### Reflection Secure FTP

La utilidad Reflection Secure FTP soporta funcionalidad cliente para FTP estándar, SFTP, y FTP/S sobre protocolos aceptables de seguridad, incluyendo SSH y SSL/TLS.

### Reflection for the Web

Reflection for the Web soporta encriptación del flujo de datos de la terminal por medio de protocolos aceptables de seguridad, incluyendo SSH y SSL/TLS.

Además, Reflection for the Web incluye al Reflection Security Proxy, que permite un acceso host amigable con el firewall. Los hosts están ocultos tras el firewall y el proxy, y múltiples hosts pueden ser accedidos por medio de un solo puerto en el firewall.

### Reflection for Secure IT

Los servidores SSH en Reflection for Secure IT proporcionan mecanismos del lado del servidor para soportar conectividad SSH desde los clientes de emulación de terminal y transferencias de archivo de Reflection.

### Requerimiento 2: No usar las contraseñas del sistema y ni otros parámetros de seguridad suministrados por default por los vendedores de software

La Sección 2.3 requiere que todo el acceso administrativo que no sea por consola a sistemas clave sea encriptado. SSH y SSL/TLS son listados como protocolos aceptables.

A continuación cómo los productos Reflection facilitan el cumplimiento con el Requerimiento 2:

### Reflection for Windows

Los productos Reflection for Windows pueden ser utilizados para acceso administrativo que no sea por consola a sistemas host. Todos soportan encriptación del flujo de datos de la terminal por medio de protocolos aceptables de seguridad, incluyendo SSH y SSL/TLS.

### Reflection for the Web

Reflection for the Web soporta la encriptación del flujo de datos de la terminal por medio de protocolos aceptables de seguridad, incluyendo SSH y SSL/TLS.

Reflection Security Proxy también proporciona conexiones encriptadas a sistemas host, como Unisys, que carecen de soporte nativo de encriptación.

### **Reflection for Secure IT**

Los clientes Secure Shell de Reflection for Secure IT ofrecen utilerías para tareas remotas de administración, ya sean interactivas o por medio de scripts, sobre el protocolo SSH.

Los servidores SSH en Reflection for Secure IT proporcionan mecanismos del lado del servidor para soportar conectividad SSH desde los clientes de emulación de terminal y transferencias de archivo de Reflection.

### **Requerimiento 3: Proteger los Datos del Tarjetahabiente**

La Sección 3.3 estipula que los números primarios de cuenta (PANs) deben estar enmascarados cuando son desplegados.

A continuación cómo Reflection® for IBM® 2007, un emulador de terminal basado en Windows, facilita el cumplimiento con el Requerimiento 3:

#### **Reflection for IBM 2007**

Reflection for IBM 2007 incluye filtros de privacidad configurables que pueden enmascarar PANs desplegados en ventanas de historial, reportes impresos y recortes.

Nota: El software de emulación de terminal Attachmate EXTRA! ofrece las mismas capacidades.

### **Requerimiento 4: Encriptar los datos del tarjetahabiente e información confidencial transmitida a través de redes públicas**

El Requerimiento 4 estipula que “La información confidencial debe encriptarse durante su transmisión a través de red, ya que es fácil y común que un delincuente intercepte y/o redirija los datos mientras se encuentran en tránsito.” La Sección 4.1 continúa especificando que deben ser utilizados robustos protocolos de seguridad y criptografía para salvaguardar la información confidencial en tránsito del tarjetahabiente.

A continuación cómo los productos Reflection facilitan el cumplimiento con el Requerimiento 4:

#### **Todos los productos Reflection**

Todas las implementaciones de los protocolos SSH y SSL/TLS en los productos Reflection usan una robusta criptografía—incluyendo los algoritmos Triple DES y AES—para encriptar la información del tarjetahabiente que es enviada sobre la red. En la mayoría de los casos, estas implementaciones criptográficas han sido validadas con FIPS 140-2 por un evaluador externo acreditado.

### **Requerimiento 6: Desarrollar y mantener sistemas y aplicaciones seguras**

La Sección 6.1 del PCI DSS requiere que usted instale los parches de seguridad más recientes que provea el vendedor de software dentro del primer mes de su publicación.

Para mantener el paso frente al panorama rápidamente cambiante de las amenazas a la seguridad, usted necesita asociarse con un vendedor que monitoree los principales servicios de alertas de seguridad y que le notifique cuando se anuncien vulnerabilidades de seguridad relevantes.

Los expertos en seguridad de Attachmate mantienen una serie de notas técnicas, disponibles en nuestro sitio de soporte, que describen las vulnerabilidades de seguridad publicadas. Si un producto Attachmate es afectado, los clientes con el plan de Mantenimiento Attachmate pueden descargar los parches de seguridad apropiados. El equipo de soporte técnico de Attachmate está también disponible para ayudarle a lidiar con cualquier problema de seguridad que surja en nuestros productos.

### **Requerimiento 7: Restringir el acceso a los datos tomando como base la necesidad de conocer la información**

Este requerimiento dictamina que solo los usuarios cuyo trabajo requiere de acceso a la información del tarjetahabiente se les pueden otorgar dicho acceso, y que la configuración por default para los usuarios, a menos de que otra cosa sea permitida, debe establecerse como “denegar todo”.

A continuación cómo Reflection for the Web facilita el cumplimiento con el Requerimiento 7:

#### **Reflection for the Web**

Todos los sistemas host ofrecen algún nivel de autorización y control de acceso. Usted puede agregar una capa adicional de seguridad con Reflection for the Web, que le permite controlar las utilerías, como los emuladores de terminal y las utilerías de transferencia de archivos, que acceden a sus hosts.

Así es como funciona: A los usuarios se les requiere registrarse dentro de un sitio web que proporciona enlaces a las sesiones de emulación de terminal y de transferencia de archivos. Las sesiones de acceso y autenticación pueden ser manejados por medio de su directorio existente de control de acceso (p. e., Active Directory). Usted puede controlar el acceso a nivel de grupo o usuario. La configuración por default en Reflection for the Web denegará el acceso a los usuarios no autorizados.

### **Requerimiento 8: Asignar una Identificación única a cada persona que tenga acceso a una computadora**

Cayendo bajo el objetivo de “implementar un fuerte control de acceso,” este Requerimiento especifica

que los usuarios deben identificarse antes de recibir el acceso a la información de los tarjetahabientes. También especifica el soporte para una variedad de metodologías de autenticación y la utilización de la autenticación doble para el acceso remoto.

A continuación cómo Reflection for the Web facilita el cumplimiento con el Requerimiento 8:

#### **Reflection for the Web**

Al poner una capa de autenticación y autorización en frente del acceso a la emulación de terminal y las utilerías para la transferencia de archivos, Reflection for the Web permite que se puedan asignar IDs únicos dentro de un directorio de usuarios existente para ser usado para el control de acceso.

Además de la autenticación basada en contraseñas, Reflection for the Web también soporta certificados digitales y claves públicas para la autenticación.

#### **Requerimiento 10: Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes**

Los mecanismos de rastreo y la habilidad de dar seguimiento a las actividades del usuario son críticas para el cumplimiento con el PCI DSS. El Requerimiento 10 rige qué eventos serán registrados con fines de auditoría y qué puntos específicos de datos son capturados en el evento registrado.

A continuación cómo los productos Reflection facilitan el cumplimiento con el Requerimiento 10:

#### **Reflection for Secure IT**

Como un proveedor de servicios Secure Shell basados en servidor, Reflection for Secure IT ofrece robustas capacidades de registro. Los eventos clave en la operación de los servidores Reflection for Secure IT, incluyendo conexiones cliente entrantes y autenticaciones, son registrados en una gran variedad de sistemas configurables, incluyendo los registros de evento estándar del sistema operativo.

#### **Reflection for the Web**

Durante las sesiones de emulación de terminal y transferencia de archivos, Reflection for the Web registra los eventos de acceso entrantes y detalla acerca de los sistemas host a los que los usuarios se están conectando.

### **Más capacidades, Cumplimiento Más Rápido**

Cumplir con el amplio rango de requerimientos del PCI DSS no es fácil. La implementación puede cruzar los límites de los departamentos, involucrar a varios equipos de gente, y afectar a múltiples plataformas de sistema. El esfuerzo requerido puede ser costoso y consumir tiempo.

Desafortunadamente, no hay una sola solución de seguridad que pueda cubrir todas sus necesidades de cumplimiento con PCI. Pero los productos Reflection, que ofrecen más capacidades de cumplimiento con PCI que cualquier otra solución de emulación de terminal, puede proporcionar una amplia base de soporte. Con herramientas que residen tanto en servidores como en las workstations de los usuarios, los productos Reflection han sido creados para reducir el tiempo que le tomará cumplir, además de poder compartir información de manera más segura.

Y hay más buenas noticias: Una vez que usted haya cumplido exitosamente sus requerimientos PCI, su organización estará en la ruta hacia el cumplimiento de otras, nuevas regulaciones.

### **La Conexión NetIQ**

Los productos Reflection descritos en este informe encajan dentro de una estrategia bien planeada de cumplimiento con PCI. Cuando se trata de manejar, monitorear y cumplir con todo el conjunto de requerimientos PCI DSS, NetIQ, una compañía de Attachmate, puede ayudar.

NetIQ es un líder en cumplimiento, monitoreo y automatización de procesos IT. Calificado por Gartner en el nivel más alto en soluciones de seguridad, NetIQ proporciona tecnología de protección y monitoreo (incluyendo SIEM) a muchas de las compañías más grandes del mundo así como a los gobiernos de varios países.

Cubriendo áreas críticas como son la seguridad del sistema, monitoreo de red, administración de directivas y control de acceso, las soluciones de NetIQ permiten un rápido desarrollo, y está listo para comenzar, en cuanto se instala el producto para auxiliarlo en sus esfuerzos de cumplimiento. Además, los expertos en seguridad de NetIQ trabajarán con su IT y su personal de cumplimiento para ajustar una solución que cumpla con sus metas específicas y se adapte a su infraestructura actual.

Para más información acerca de las soluciones NetIQ, visite [www.netiq.com](http://www.netiq.com).



**Sede Central**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL +1 206 217 7500  
FAX +1 206 217 7515

**Oficina Central Para América Latina**  
México  
TEL +52 55 9178 4970  
FAX +52 55 5540 4886

**Oficina Central Para EMEA**  
Países Bajos  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Oficina Central Para España**  
Madrid  
TEL +34 911517111  
TEL +34 911517120

WEB [www.attachmate.com.mx](http://www.attachmate.com.mx)  
EMAIL [marketingmex@attachmate.com](mailto:marketingmex@attachmate.com)

Para obtener información sobre las oficinas regionales, visite [www.attachmate.com.mx](http://www.attachmate.com.mx).

Proporcionado solo con fines informativos; puede ser modificado en cualquier momento sin previo aviso.  
Copyright © 2009 Attachmate Corporation. Todos los derechos reservados. Attachmate, el logo Attachmate, Reflection y EXTRA! son nombres o marcas registradas de Attachmate Corporation, en EU y otros países. INFOConnect es una marca registrada de Unisys Corporation. Windows es una marca registrada de Microsoft Corporation en EU y otros países. IBM es una marca registrada de International Business Machines Corporation. Las especificaciones de PCI DSS, incluyen lista de 12 Requerimientos PCI, Consejo de Estándares de Seguridad © 2006 — 2008 PCI, LLC. Todas las otras marcas, nombres comerciales o nombres de compañías hechas referencia aquí son solo usados con fines de identificación y son propiedad de sus respectivos dueños. 08-0014S.0109