

Cumplimiento del Estándar de Seguridad de Datos de la Industria de Pagos con Tarjeta

Soluciones de Datos Empresariales Seguros para los Requerimientos 3 y 4 de PCI DSS



The Security Division of EMC

Un pilar central de la norma de la Industria de pagos con tarjeta (PCI, *Payment Card Industry*), detallada en el Requerimiento 3, es que las organizaciones deben proteger los datos que poseen de los titulares de tarjetas, independientemente de dónde se encuentre la información, ya sea en las terminales de puntos de venta, en las bases de datos locales o centrales, en los archivos y carpetas, en el almacenamiento de información o en otro sitio. Además, la norma de seguridad de datos (DSS, *Data Security Standard*) PCI establece, mediante el Requerimiento 4, que los negocios deben proteger los datos de las tarjetas a medida que cruzan la red y se mueven entre los sistemas y las aplicaciones.

Al requerir que las organizaciones empleen un enfoque centrado en la información, que garantiza la protección de los datos, la PCI DSS obliga a las empresas a ir más allá del perímetro y examinar los mecanismos para proteger los datos en todo el ciclo de vida de la información.

Administración de los Requerimientos de Encriptación y Más

Las directivas definidas en los Requerimientos 3 y 4 de PCI DSS son explícitas, pero las implicaciones que van más allá de las establecidas en la norma son mucho más amplias. Cuando las organizaciones comienzan a encriptar datos en diversos sistemas, se hace evidente el desafío de la administración de claves de encriptación.

A fin de afrontar los desafíos de administración de claves y encriptación, RSA ofrece una amplia gama de soluciones de protección de datos empresariales. Con el respaldo del software RSA Key Manager que se encarga de la administración de claves en toda la empresa, RSA permite a los clientes garantizar que las soluciones de protección de datos puedan escalarse y adaptarse a los cambios del negocio, y que sus datos estén disponibles y bien protegidos, independientemente de dónde se los necesite en el ciclo de vida de la información.

Beneficios para el Cliente: Protección de Datos Empresariales

Con las soluciones RSA para la protección de datos empresariales, podrá:

- Proteger de manera eficaz los datos de las tarjetas de crédito en cualquier parte de la empresa y administrar centralizadamente esta seguridad.
- Asegurarse de que su estrategia de protección de datos pueda escalarse y adaptarse a los cambios del negocio y, que sus datos vitales estén disponibles y protegidos, independientemente de dónde se los necesite en el ciclo de vida de la información.
- Aprovechar la escalabilidad de las soluciones de protección de datos empresariales de RSA para proteger todo tipo de información valiosa del negocio, a los clientes, a los asociados de negocios y a los empleados de toda la empresa.

Además, RSA ofrece una amplia gama de productos, entre los que se encuentran RSA® Database Security Manager y RSA® File Security Manager, que le permite a los clientes proteger la información de los titulares de tarjetas en todas las terminales de encriptación, independientemente de si la información reside en una aplicación, una base de datos, en archivos y carpetas o si está almacenada en discos o cintas.

Para obtener más información acerca de las soluciones de RSA que ayudan a los clientes a afrontar el cumplimiento de PCI DSS, visite www.rsa.com/pci.

Componentes de la Solución PCI de RSA

- > **RSA® Access Manager:** la solución de RSA para proteger el acceso Web permite que los comerciantes, los bancos y los procesadores de pagos puedan asegurarse de que solamente los usuarios con una necesidad de obtener información del negocio puedan acceder a la información de los titulares de tarjetas en sistemas PCI basados en la Web.
- > **Soluciones de Datos Empresariales Seguros de RSA:** las soluciones de datos empresariales seguros de RSA permiten que los negocios afectados por la norma PCI puedan proteger los datos de los titulares de tarjetas de crédito en todas las terminales de encriptación y administrar de manera centralizada las claves de encriptación en toda la empresa.
 - RSA Database Security Manager
 - RSA File Security Manager
 - RSA Key Manager
 - Gateway de Seguridad IP CipherOptics
 - Dispositivos de seguridad de almacenamiento de información Decru DataFort®
 - Dispositivos NeoScale CryptoStor®
- > **RSA enVision®:** la solución de RSA para el cumplimiento de normas y la administración de la información de seguridad permite a las organizaciones que se ven afectadas por PCI DSS simplificar el proceso de auditoría mediante el establecimiento de un punto centralizado para realizar el seguimiento y monitoreo del acceso a los datos de los titulares de tarjetas en todo un entorno de PCI. Monitoree el acceso a los recursos de red y a los datos de los titulares de tarjetas.
- > **RSA SecurID®:** las soluciones de RSA para proteger el acceso a los datos empresariales permiten a los clientes asegurarse de que los usuarios que acceden a los sistemas de datos de titulares de tarjetas y a la red informática en general son quienes dicen ser.
- > **RSA Professional Services:** RSA Professional Services ofrece diversas capacidades que permiten a los clientes prepararse para una auditoría de PCI DSS, soportar el descubrimiento de la amplia base de datos de los titulares de tarjetas en toda la empresa e implementar tecnologías de reparación.
- > **Celerra® y Centera®** de EMC: la integración incorporada de Celerra y Centera de EMC con la tecnología RSA enVision permite a los clientes almacenar de manera rentable los datos críticos del log de auditoría de PCI.

Requerimiento 3 de PCI DSS: Proteger la información almacenada de los titulares de tarjetas

Requerimiento 4 de PCI DSS: Encriptar la transmisión de la información de los titulares de tarjetas en las redes públicas y abiertas

RSA ofrece una amplia gama de tecnologías de protección de datos empresariales que permiten a los clientes afrontar los requerimientos 3 y 4 de PCI DSS al proteger los datos de los titulares de tarjetas dondequiera que residan en la organización. Las ofertas de RSA permiten que los clientes protejan los datos de los titulares de las tarjetas de crédito en todas las terminales de encriptación, independientemente de si la información reside en una aplicación, una base de datos, en archivos y carpetas o si está almacenada en discos o cintas, y que administren de manera centralizada las claves de encriptación de toda la empresa. Las funcionalidades específicas que ofrece RSA para afrontar la norma PCI DSS comprenden:

Requerimientos de PCI DSS Capacidad de RSA

<p>Requerimiento 3.4: Hacer que el número de cuenta principal (PAN, <i>Primary Account Number</i>), como mínimo, no pueda ser leído en cualquier lugar en donde esté almacenado (datos en medios digitales portátiles, medios de backup, en registros y datos recibidos en las redes inalámbricas o almacenados por estas redes) mediante el uso de cualquiera de los siguientes enfoques:</p> <ol style="list-style-type: none">1) Funciones sólidas de ordenamiento unidireccionales (índices de ordenamiento)2) Truncamiento3) Bases y tokens de indexación (las bases deben estar almacenadas de forma segura)4) Criptografía sólida con procedimientos y procesos de administración de claves asociados. La información mínima sobre la cuenta que debe hacerse ilegible es el número de cuenta personal o PAN.	<p>RSA Key Manager proporciona bibliotecas de desarrollo de aplicaciones que soportan una gran variedad de lenguajes de desarrollo, y ayuda a los desarrolladores a integrar fácilmente la encriptación en un punto de venta, pago, CRM, ERP y otras aplicaciones que creen o procesen información confidencial.</p> <p>RSA Database Security Manager permite a los clientes encriptar información en el nivel de la base de datos y soporta una amplia gama de sistemas de administración de bases de datos (DBMS), incluso SQL Server, IBM DB/2, Sybase y Teradata.</p> <p>RSA Database Security Manager es particularmente eficaz para las organizaciones con entornos de DBMS heterogéneos, ya que la tecnología le permite a las empresas hacer cumplir políticas de seguridad consistentes en diversos sistemas DBMS.</p> <p>RSA File Security Manager ofrece a los clientes la posibilidad de proteger contra ataques internos y externos los datos de las tarjetas de crédito en archivos en computadoras de escritorio, computadoras portátiles y servidores. Además, permite que los clientes administren y cumplan de manera centralizada la separación de tareas, junto con otras políticas de seguridad, para archivos confidenciales, independientemente de dónde se encuentren en la red.</p> <p>A través de la asociación con Decru y NeoScale Systems, RSA ofrece capacidades de encriptación para los sistemas de cinta y almacenamiento de información en discos. Los dispositivos de seguridad de almacenamiento de información Decru DataFort® permiten a los clientes automatizar y simplificar la administración segura de datos para entornos empresariales heterogéneos, en especial, en entornos de almacenamiento de información en disco SAN/NAS complejos. Los dispositivos NeoScale CryptoStor® automatizan la encriptación de datos que se encuentran en una red de almacenamiento de información o en reposo en discos, cintas virtuales o medios de cinta.</p>
<p>Requerimiento 3.5: Proteger claves de encriptación utilizadas para encriptar la información de los titulares de tarjetas contra la divulgación o el uso indebido.</p>	<p>RSA Key Manager es una tecnología de administración de claves de encriptación centralizada que les permite a las empresas cumplir las políticas de forma centralizada en toda la organización. Además, la tecnología permite a los clientes restringir el acceso a las claves y almacenar de manera segura las claves de encriptación. Al integrarse con las tecnologías de encriptación de RSA, así como con tecnologías de terceros como Decru y NeoScale, RSA proporciona una plataforma común para reforzar la seguridad de la información de los titulares de tarjetas. Además, RSA se asociará con Epicor CRS para integrar RSA Key Manager con la solución de puntos de venta CRS RetailStore™ a fin de ayudar a proteger la información confidencial, como los datos de las tarjetas de crédito, en el punto de entrada.</p>
<p>Requerimiento 3.5.1: Restringir el acceso a las claves a la menor cantidad de custodios necesarios.</p>	<p>El software RSA Key Manager permite a los clientes restringir el acceso a las claves de encriptación al garantizar que los usuarios estén correctamente autenticados y autorizados, controles que los auditores de PCI DSS esperan corroborar.</p>
<p>Requerimiento 3.5.2: Almacenar claves de forma segura en la menor cantidad posible de ubicaciones y formas.</p>	<p>RSA Key Manager almacena las claves de encriptación en una base de datos consolidada (el almacenamiento de claves) donde se encriptan las claves en sí con una clave de encriptación de claves (KEK, <i>Key Encryption Key</i>). Los clientes tienen la capacidad de almacenar esta KEK en un módulo de seguridad de hardware (HSM, <i>Hardware Security Module</i>), un dispositivo de hardware seguro y especializado que respalda la protección de todas las claves de encriptación de la empresa.</p>
<p>Requerimiento 3.6: Documentar e implementar de manera completa todos los procesos y procedimientos de administración de claves en relación con las claves utilizadas para la encriptación de la información de los titulares de tarjeta, incluso lo siguiente:</p>	<p>RSA Key Manager proporciona un fuerte soporte para la administración de claves de encriptación a lo largo de todo el ciclo de vida, desde la creación de claves seguras hasta la protección del almacenamiento y la distribución de claves y el hecho de hacer que las claves de encriptación sean virtualmente inaccesibles.</p>

Continúa de la página anterior

Requerimientos de PCI DSS	Capacidad de RSA
<p>Requerimiento 3.6.1: Generación de claves seguras. Requerimiento 3.6.2: Distribución segura de claves. Requerimiento 3.6.3: Almacenamiento seguro de claves.</p>	<p>RSA Key Manager brinda a las empresas la capacidad de generar claves seguras y de proteger tanto la distribución como el almacenamiento de las claves.</p>
<p>Requerimiento 3.6.4: Cambio periódico de claves: 1) Según lo considere necesario o lo recomiende la aplicación asociada (por ejemplo, volver a especificar una clave); preferentemente de manera automática. 2) Al menos una vez al año.</p>	<p>RSA Key Manager ayuda a los clientes a modificar periódicamente las claves de acuerdo con la política implementada para proteger los datos de los titulares de tarjetas en todo el entorno del cliente.</p>
<p>Requerimiento 3.6.5: Destrucción de claves antiguas.</p>	<p>RSA Key Manager permite a los clientes destruir claves de encriptación antiguas.</p>
<p>Requerimiento 3.6.6: Separación del conocimiento y establecimiento del control dual de claves (de modo que se requieran dos o tres personas y que cada una sepa su parte de la clave, a fin de reconstruir la clave completa).</p>	<p>RSA Key Manager supera este requisito al hacer prácticamente imposible acceder a las claves. Almacena las claves de encriptación en un almacén de claves consolidado donde las claves se encriptan con una clave de encriptación de claves (KEK). Esta KEK puede almacenarse en un módulo de seguridad de hardware (HSM, <i>Hardware Security Module</i>), un dispositivo de hardware seguro y especializado que respalda la protección de todas las claves de encriptación de la empresa. Las tecnologías de control de acceso refuerzan aún más la protección de las claves de encriptación y KEK.</p>
<p>Requerimiento 3.6.7: Prevención de reemplazo de claves sin autorización.</p>	<p>RSA Key Manager permite a los clientes evitar el reemplazo no autorizado de claves al garantizar que sólo las aplicaciones con doble autenticación puedan solicitar claves y que sólo se utilicen para encriptar datos aquellas claves que se adapten a la política definida para esas aplicaciones. Las normas para elegir claves están determinadas por políticas y no se permite la intervención de los usuarios en este proceso.</p>
<p>Requerimiento 3.6.8: Reemplazo de claves que se sospecha que están comprometidas o que se sabe que lo están.</p>	<p>RSA Key Manager permite a los clientes reemplazar claves que se sospecha que están comprometidas o que se sabe que lo están.</p>
<p>Requerimiento 3.6.9: Revocación de claves antiguas o no válidas.</p>	<p>RSA Key Manager permite a los clientes revocar claves antiguas o no válidas.</p>
<p>Requerimiento 3.6.10: Los custodios de claves deben firmar un formulario en el que se establece que comprenden y aceptan sus responsabilidades como custodios de claves.</p>	<p>RSA Key Manager puede relegar los custodios de claves al punto en el que un custodio jamás podría acceder a una clave. Los custodios pueden administrar políticas asociadas con las claves, pero no pueden “modificar” las claves en sí. Esta capacidad supera el requerimiento de PCI.</p>
<p>Requerimiento 4.1: Utilizar protocolos de seguridad y criptografía sólidos, tales como Secure Sockets Layer (SSL)/Transport Layer Security (TLS) y el Protocolo de seguridad de Internet (IPSEC) para proteger la información confidencial de los titulares de tarjetas durante la transmisión de dicha información a través de redes públicas y abiertas. Entre los ejemplos de redes abiertas públicas que están dentro del alcance de PCI DSS se encuentran Internet, WiFi (IEEE 802.11x), sistema mundial de comunicaciones móviles (GSM) y servicio general de paquetes por radio (GPRS).</p>	<p>Gracias a su asociación con CipherOptics, RSA ofrece un método transparente de seguridad para los datos en tránsito entre redes IP internas, lo cual ayuda a proteger los enlaces entre los sistemas y garantiza así que los datos confidenciales no puedan ser alterados al recorrer dichos sistemas. RSA Key Manager proporciona un fuerte soporte para la administración de claves de encriptación a lo largo de todo el ciclo de vida, desde la creación de claves seguras hasta la protección del almacenamiento y la distribución de claves y el hecho de hacer que las claves de encriptación sean virtualmente inaccesibles.</p>
<p>Requerimiento 4.1.1: Para redes inalámbricas que transmitan información de los titulares de tarjetas, encriptar las transmisiones mediante tecnología de acceso WiFi protegido (WPA o WPA2), IPSEC VPN o SSL/TLS. Nunca confíe exclusivamente en el protocolo wired equivalent privacy (WEP) para proteger la confidencialidad y acceder a una LAN inalámbrica.</p>	<p>El producto IP Security Gateway de CipherOptics proporciona a los clientes la capacidad de encriptar datos en tránsito sin importar el tipo de red sobre la cual se transmita la información.</p>



RSA Security Inc.
 RSA Security Ireland Limited
www.rsa.com

©2007 RSA Security Inc. Todos los derechos reservados. RSA, RSA Security, enVision, SecurID y el logotipo de RSA son marcas comerciales registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC, Celerra y Centera son marcas comerciales de EMC Corporation. Todos los demás productos y servicios mencionados son marcas comerciales de sus respectivas empresas.