

Cumplimiento de Normas y Administración de Información de Seguridad para el Requerimiento 10 de PCI DSS y Más



El Estándar de Seguridad de Datos (DSS, *Data Security Standard*) de la Industria de Pagos con Tarjeta (PCI, *Payment Card Industry*) impone una amplia gama de requerimientos de reporting, que resultan de primordial importancia durante las auditorías anuales de PCI DSS. Además, mediante el Requerimiento 10, PCI DSS específicamente requiere a comerciantes, bancos y procesadores de pago que “realicen un seguimiento de todo el acceso a los recursos de la red y a la información de los titulares de tarjetas”.

A medida que los negocios toman distancia y reconocen las implicaciones del reporting y monitoreo de PCI DSS, surgen los siguientes interrogantes: “Mientras el cumplimiento de normas sea crítico, ¿cómo puede mi organización ser más proactiva que reactiva, y cómo podemos garantizar que el tiempo y los recursos invertidos se extiendan más allá de la iniciativa de PCI DSS?”.

Tecnología de RSA enVision® para Ir Más Allá del Cumplimiento de Normas

Las violaciones de políticas y seguridad ocurren sin previo aviso. Independientemente de que se trate de errores accidentales o de intentos de acceder a información privada de manera ilegal, se necesita visibilidad inmediata respecto de estos comportamientos para poder responder a ellos. La visibilidad y la capacidad de respuesta son críticas para lograr el cumplimiento de normas de PCI DSS y, desde una perspectiva más amplia, son necesarias para garantizar la seguridad de toda la información de asociados de negocios, clientes y negocios privados de su organización.

RSA enVision transforma eventos raw de seguridad y de red aparentemente no relacionados en inteligencia del negocio significativa. RSA enVision establece, en primer lugar, niveles de base para la actividad de todo el entorno de red, por lo que permite determinar comportamientos irregulares y emitir alertas cuando ocurren este tipo de actividades. Al capturar todos los datos, desde aplicaciones empresariales, de red y de seguridad hasta dispositivos de mainframe, de escritorio y de almacenamiento de información, RSA enVision garantiza una visibilidad completa y sin filtros.

Beneficios para el Cliente: Solución de Administración de la Información de Seguridad y de Cumplimiento de Normas

Con la tecnología de RSA enVision podrá:

- Tener la certeza de que, cuando se produzca una violación de seguridad o de una política, sabrá cómo responder.
- Volver a concentrarse en el crecimiento de su negocio, en lugar de responder a auditorías, porque su organización cuenta con una herramienta que permite demostrar rápidamente el cumplimiento con los requerimientos clave de PCI DSS.
- Ir más allá del cumplimiento de normas al aprovechar las inversiones basadas en PCI DSS para mejorar la posición de seguridad general de su compañía.

Además del cumplimiento de normas de PCI, RSA enVision elimina los silos de datos del negocio que pueden crearse en muchas organizaciones. RSA enVision recopila, analiza y administra todos los datos, y proporciona una plataforma que permite informar a prácticamente todas las personas de su organización. Los auditores de cumplimiento de normas contarán con un conjunto completo de datos para enfrentar problemas de cumplimiento, y el personal de administración de riesgos y el sector de operaciones de seguridad podrán ver las alertas de seguridad en tiempo real. Todos, desde la gente de operaciones y de la mesa de ayuda hasta el personal de administración de redes y aplicaciones, podrán acceder a los informes que necesiten en cualquier momento.

RSA enVision aprovecha Internet Protocol Database (IPDB) de LogSmart para recopilar y analizar la información de seguridad y cumplimiento de normas de su compañía. IPDB de LogSmart mantiene una cadena de custodia digital de todos los datos que asegura que, una vez que se asignan los datos a la base de datos, no se puedan alterar más, a diferencia de la mayoría de los esquemas de datos utilizados en soluciones basadas en sistemas de administración de bases de datos relacionales (RDBMS, *Relational Database Management System*).

Componentes de la Solución PCI de RSA

- > **RSA® Access Manager:** la solución de RSA para proteger el acceso a empresas 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 RSA Enterprise Data Protection.** 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 titulares de tarjetas en todo un entorno de PCI.
- > **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 las tarjetas en toda la empresa e implementar tecnologías de reparación.
- > **Celerra de EMC y Centera de EMC:** la integración incorporada de Celerra de EMC 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.

Además, mientras que otras soluciones reducen o filtran de antemano los datos provenientes de dispositivos de origen, simplemente porque el RDBMS no puede mantenerse a la par, RSA enVision captura el conjunto completo de datos de IPDB de LogSmart. Su organización obtendrá los beneficios del análisis en tiempo real y la autenticación paralela y compresión de datos de origen, lo que significa que las alertas son altamente precisas y oportunas. Los beneficios de la recopilación sin agentes son evidentes: ausencia de filtro de datos en el origen, ausencia de administración continua de agentes distribuidos en toda la red, una infraestructura de red sin riesgos ni impactos y un menor costo total de propiedad debido a la facilidad de configuración e implementación.

Finalmente, la tecnología RSA enVision posiciona a su negocio para que responda inmediatamente a las violaciones de políticas y seguridad, lo que ayuda a mejorar la posición de seguridad de TI de la organización y simplifica el proceso de cumplimiento de normas.

RSA enVision ayuda a posicionar a los clientes para que se concentren en los recursos humanos y financieros de las iniciativas de crecimiento del negocio, en lugar de reaccionar a un ciclo constante de auditorías de PCI DSS.

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

Requerimiento 10 de PCI DSS y RSA enVision

El requerimiento 10 de PCI DSS establece que las empresas deben “monitorear y realizar un seguimiento de todo el acceso a los recursos de la red y a los datos de titulares de tarjetas”. RSA enVision permite a los clientes simplificar el proceso de auditoría mediante el establecimiento de un punto centralizado para el seguimiento y monitoreo del acceso a datos de titulares de tarjetas en un entorno de PCI. Las capacidades específicas que ofrece RSA enVision para enfrentar la norma PCI DSS incluyen:

Requerimiento 10 de PCI DSS y RSA enVision

REQUERIMIENTOS DE PCI DSS	CAPACIDAD DE RSA enVISION
<p>> Requerimiento 10.1 Establecer un proceso para vincular todo el acceso a los componentes del sistema (especialmente el acceso realizado con privilegios administrativos, por ejemplo, de raíz) con cada usuario individual</p>	<p>RSA enVision permite a los clientes realizar un seguimiento de la actividad administrativa de los usuarios y proporciona un control para comprobar si un usuario está actuando de acuerdo con la política establecida. Además, el sistema puede enviar una alerta al supervisor del usuario si los comportamientos violan la política.</p> <p>RSA enVision ofrece reporting “listo para usar” que muestra todos los escalamientos exitosos de privilegios administrativos en sistemas UNIX y Linux monitoreados.</p> <p>Informe: “PCI: Escalamiento de Privilegios Administrativos, Unix y Linux”</p>
<p>> Requerimiento 10.2 Implementar pistas de auditoría automatizadas para todos los componentes del sistema con el objetivo de reconstruir los siguientes eventos</p>	<p>El dispositivo RSA enVision ayuda a las empresas a implementar pistas de auditoría automatizadas, las cuales describen el acceso de los usuarios a la información de los titulares de tarjetas, las acciones de usuarios con privilegios administrativos y de raíz, el acceso a las pistas de auditoría, los intentos de acceso lógicos no válidos, el uso de los mecanismos de identificación/autenticación, la inicialización de los logs de auditoría y la creación y eliminación de objetos en el nivel del sistema.</p>
<p>Requerimiento 10.2.1 Todos los accesos de usuarios individuales a la información de los titulares de tarjetas</p>	<p>RSA enVision ofrece capacidades de reporting integradas que muestran todos los intentos exitosos de acceso a archivos para almacenar objetos en el grupo de dispositivos de “datos de titulares de tarjetas”. Este grupo de dispositivos constituye un subconjunto de grupos de dispositivos PCI y debe contener únicamente los servidores utilizados en el almacenamiento de datos de titulares de tarjetas.</p> <p>Informe: “PCI: Accesos de Usuarios Individuales a la Información de los Titulares de Tarjetas, Windows”</p>
<p>Requerimiento 10.2.2 Todas las acciones realizadas por individuos con privilegios administrativos o de raíz</p>	<p>RSA enVision permite que los clientes informen todas las acciones realizadas por usuarios que hayan iniciado sesión con privilegios de “raíz”. Además, las organizaciones pueden personalizar este informe para incluir cualquier nombre de usuario adicional al que se haya otorgado privilegios administrativos completos de monitorio de usuarios en su entorno.</p> <p>Informe: “PCI: Todas las Acciones de Individuos con Privilegios Administrativos o de Raíz, Unix y Linux”</p> <p>El reporting de RSA enVision permite que los clientes monitoreen todas las acciones realizadas por los usuarios que hayan iniciado sesión como “Administrador”. Los clientes pueden reforzar aún más la seguridad al incluir cualquier nombre de usuario adicional al que se haya otorgado privilegios administrativos completos en su entorno.</p> <p>Informe: “PCI: Todas las Acciones de Individuos con Privilegios Administrativos o de Raíz, Windows”</p>
<p>Requerimiento 10.2.3 Acceso a todas las pistas de auditoría</p>	<p>RSA enVision ofrece informes integrados que permiten a los clientes monitorear fácilmente todos los inicios de sesión exitosos en RSA enVision.</p> <p>Informe: “PCI: Acceso a Todas las Pistas de Auditoría”</p>
<p>Requerimiento 10.2.4 Intentos de acceso lógico no válidos</p>	<p>RSA enVision permite que los clientes informen fácilmente todos los intentos de acceso denegados debido a las restricciones de la lista de control de acceso.</p> <p>Informe: “PCI: Intentos de Acceso Lógico no Válidos, Resumen Denegado por Lista de Control de Acceso (ACL)”</p>
<p>Requerimiento 10.2.5 Uso de mecanismos de identificación y autenticación</p>	<p>RSA enVision permite que las organizaciones vean fácilmente un informe que detalle el acceso de todos los usuarios al grupo de dispositivos PCI de autenticación mediante servidores RSA Authentication Manager.</p> <p>Informe: “PCI: Uso de Sistemas de Identificación y Autenticación, RSA”</p>
<p>Requerimiento 10.2.6 Inicialización de logs de auditoría</p>	<p>RSA enVision ofrece informes “listos para usar” que proporcionan una vista de la inicialización de logs de auditoría en sistemas operativos Windows, UNIX, Linux, AIX y HP-UX.</p> <p>Informe: “PCI: Inicialización de Logs de Auditoría”</p>
<p>Requerimiento 10.2.7 Creación y eliminación de objetos en el nivel del sistema</p>	<p>Las capacidades de reporting de RSA enVision permiten a los clientes ver la eliminación de todos los objetos en el nivel del sistema de sistemas Windows monitoreados, que se ejecutan en el grupo de dispositivos “PCI”.</p> <p>Informe: “PCI: Eliminación de Objetos en el Nivel del Sistema, Windows”</p>

Requerimiento 10 de PCI DSS y RSA enVision (continuación)

REQUERIMIENTOS DE PCI DSS	CAPACIDAD DE RSA ENVISION
<p>> Requerimiento 10.3 Registrar, como mínimo, las siguientes entradas de pistas de auditoría de todos los componentes del sistema para cada evento</p>	<p>RSA enVision registrará los eventos tal como los informan los dispositivos asociados. Además, RSA enVision guarda los metadatos de los eventos, que se pueden analizar y revisar para determinar el tipo de evento.</p>
<p>Requerimiento 10.3.1 Identificación de usuario</p>	<p>RSA enVision permite que las organizaciones registren información de identificación de usuario para cada evento asociado con el grupo de dispositivos PCI.</p>
<p>Requerimiento 10.3.2 Tipo de evento</p>	<p>RSA enVision permite que las organizaciones identifiquen información de tipo de evento para cada evento asociado con el grupo de dispositivos PCI. Si el dispositivo no informa el tipo de evento, de todas maneras RSA enVision proporciona soporte para el reporting al guardar metadatos que se pueden analizar y revisar para determinar el tipo de evento.</p>
<p>Requerimiento 10.3.3 Fecha y hora</p>	<p>RSA enVision permite que las organizaciones registren información de fecha y hora para cada evento asociado con el grupo de dispositivos PCI.</p>
<p>Requerimiento 10.3.4 Indicación de éxito o falla</p>	<p>RSA enVision permite que las organizaciones registren información de indicación de éxito o falla para cada evento asociado con el grupo de dispositivos PCI.</p>
<p>Requerimiento 10.3.5 Origen del evento</p>	<p>RSA enVision permite que las organizaciones registren información de origen del evento para cada evento asociado con el grupo de dispositivos PCI.</p>
<p>Requerimiento 10.3.6 Identidad o nombre de los datos, los componentes del sistema o los recursos afectados</p>	<p>RSA enVision permite a las organizaciones registrar el nombre u otra identidad de sistemas, datos, componentes, u otros recursos de PCI afectados.</p>
<p>> Requerimiento 10.5 Proteger las pistas de auditoría para que no se puedan alterar</p>	<p>RSA enVision ofrece datos espejados sin filtrar a su Base de datos de protocolos de Internet, que ofrece la capacidad de conservar los datos en su formato original. Además, la funcionalidad “una escritura, muchas lecturas” ayuda a garantizar que la copia espejada permanezca intacta, incluso si los datos originales se ven comprometidos. Los logs de eventos capturados por RSA enVision se almacenan en un sistema operativo consolidado de forma comprimida y se encuentran protegidos mediante una encriptación sencilla.</p>
<p>Requerimiento 10.5.1 Limitar la vista de pistas de auditoría a aquellas personas con una necesidad relacionada con el trabajo</p>	<p>RSA enVision permite a las organizaciones asignar privilegios, de modo que sólo los usuarios autorizados puedan acceder a la pista de auditoría y verla.</p>
<p>Requerimiento 10.5.2 Proteger los archivos de pista de auditoría contra modificaciones no autorizadas</p>	<p>Los logs de RSA enVision no se pueden modificar mediante la interfaz gráfica de usuario (GUI, <i>Graphical User Interface</i>). Sólo se pueden efectuar cambios mediante el acceso administrativo al dispositivo de RSA enVision. Además, las APIs de archiving y el acceso a datos de RSA enVision son de sólo lectura, de modo que los logs no se pueden alterar en el sistema.</p>
<p>Requerimiento 10.5.3 Hacer backups con prontitud de archivos de pista de auditoría en un servidor de logs centralizado u otro medio que sea difícil de modificar</p>	<p>RSA enVision permite programar backups de la pista de auditoría con la frecuencia necesaria para un servidor de logs centralizado u otros medios; por ejemplo, cada 10 minutos o cada hora, en función de las necesidades del cliente.</p> <p>RSA enVision ofrece una API de “Mantenimiento de LS” que permite a los usuarios programar backups en un dispositivo o un grupo de dispositivos (por ejemplo, grupo de dispositivos PCI). Por ejemplo, los clientes podrán programar los backups de PCI cada 10 minutos, mientras que para los dispositivos fuera del alcance de PCI los backups se podrán realizar a diario.</p>

Requerimiento 10 de PCI DSS y RSA enVision (continuación)

REQUERIMIENTOS DE PCI DSS	CAPACIDAD DE RSA ENVISION
<p>Requerimiento 10.5.5 Utilizar software de detección de cambios y monitoreo de integridad de archivos en logs para garantizar que los datos de logs existentes no se pueden modificar sin generar alertas (aunque los nuevos datos que se agregan no deberían generar alertas)</p>	<p>RSA enVision permite crear alertas que garantizan que los supervisores y otras personas sepan si se efectúan cambios en los logs. Además, la tecnología RSA enVision basada en dispositivos se basa en un sistema operativo consolidado que ofrece niveles superiores de seguridad.</p>
<p>> Requerimiento 10.7 Conservar el historial de las pistas de auditoría, por lo menos durante un año, y con un mínimo de disponibilidad en línea de tres meses</p>	<p>RSA enVision NAS3500 ofrece la solución Celerra de EMC preconfigurada, probada y montada previamente de modo no visible, que permite a los clientes soportar entre 3,5 TB y 7 TB de almacenamiento de información, lo cual es muy importante para la retención de los datos de logs en línea.</p> <p>Además, debido a que RSA enVision está diseñado para ofrecer integración incorporada con plataformas de networked storage, como Centera™ de EMC® y Celerra® de EMC, los clientes pueden almacenar su información crítica para cumplir los requerimientos de cumplimiento de normas.</p> <p>Los sistemas de Almacenamiento de Información Conectado en Red Celerra de EMC ofrecen una relación precio/performance líder en la industria con disponibilidad sin comprometer los recursos. Gracias a una disponibilidad sin compromisos, las aplicaciones pueden seguir ejecutando aplicaciones con el mismo performance y niveles de servicio, incluso en el caso de una falla. Celerra logra esto mediante una arquitectura de clustering activo-pasivo N+1 y al eliminar cualquier punto único de falla de la red a la unidad de disco.</p> <p>Los sistemas de Almacenamiento de Información Conectado en Red Celerra de EMC implementan una funcionalidad denominada “Retención en el Nivel de Archivos” que ofrece protección WORM basada en discos para los archivos. Esta funcionalidad de Celerra protege los archivos y los directorios contra la eliminación, la alteración, los cambios de nombres o la sobrescritura durante el “período de retención” designado. La Retención en el Nivel de Archivos de Celerra puede proporcionarles a las organizaciones la capacidad de proteger la integridad de los logs de auditoría en línea durante un período de retención específico (por ejemplo, 3 meses).</p>

Reporting y Auditoría de PCI DSS y RSA enVision

Además de su capacidad esencial de ayudar a los clientes a enfrentar el Requerimiento 10 de PCI DSS, la tecnología RSA enVision proporciona una sólida plataforma para recopilar, correlacionar y auditar el acceso a una amplia gama de sistemas PCI, desde firewalls y redes inalámbricas hasta mecanismos de autenticación y mucho más. La tecnología ayuda a los clientes a enfrentar los requerimientos clave de PCI DSS, ya que:

- Ofrece un conjunto sólido de informes de actividad del firewall para la rápida validación del cumplimiento del Requerimiento 1 (“Instalar y mantener una configuración de firewall para proteger la información de los titulares de tarjetas”).

- Permite a los clientes enfrentar las partes clave del Requerimiento 2 (“No usar opciones predeterminadas suministradas por los proveedores para las contraseñas de los sistemas y demás parámetros de seguridad”) mediante la fácil generación de informes sobre cambios de configuración realizados en entornos inalámbricos.
- Simplifica el proceso de generación de informes sobre actualizaciones de sistemas antivirus de la empresa para respaldar el Requerimiento 5 (“Usar y actualizar de manera regular software antivirus”).
- Respalda los esfuerzos para demostrar el cumplimiento del Requerimiento 6 (“Desarrollar y mantener aplicaciones y sistemas seguros”) mediante informes sobre aplicaciones de servicio y correcciones.

Reporting y Auditoría de PCI DSS y RSA enVision

REQUERIMIENTOS DE PCI DSS

CAPACIDAD DE RSA ENVISION

> Requerimiento 1.1

Establecer estándares de configuración del firewall que incluyan lo siguiente:

<p>Requerimiento 1.1.1 Un proceso formal para la aprobación y evaluación de todas las conexiones de redes externas y los cambios de configuración del firewall</p>	<p>RSA enVision soporta el cumplimiento de normas, ya que brinda informes “listos para usar” que muestran todos los cambios de configuración realizados en firewalls del grupo de dispositivos PCI. Informe: “PCI: Modificaciones en la Configuración del Firewall”</p>
<p>Requerimiento 1.1.5 Lista documentada de servicios y puertos necesarios para el negocio</p>	<p>RSA enVision ofrece reporting incorporado para resumir todo el tráfico de firewall por puerto en el grupo de dispositivos PCI. Informe: “PCI: Tráfico por Puerto, Grupo de Dispositivos PCI”</p>
<p>Requerimiento 1.1.6 Justificar y documentar cualquier protocolo disponible, además de Hypertext Transfer Protocol (HTTP, <i>Protocolo de Transferencia de Hipertexto</i>), Secure Sockets Layer (SSL), Secure Shell (SSH) y Red privada virtual (VPN, <i>Virtual Private Network</i>)</p>	<p>RSA enVision ofrece plantillas de informes “listas para ejecutarse” que detallan todo el tráfico de firewall por puerto a la dirección IP especificada como parámetro de tiempo de ejecución en el que PCI no justifica el puerto utilizado de manera directa. Informe: “PCI: Tráfico en Puertos no Estándar, Detalle” El reporting de RSA enVision resume todo el tráfico de firewall por puerto y computadora de destino, en casos en que el PCI no justifique el puerto utilizado de manera directa. Informe: “PCI: Tráfico en Puertos no Estándar, Resumen”</p>
<p>Requerimiento 1.1.8 Revisar trimestralmente los conjuntos de reglas de router y firewall</p>	<p>El reporting de RSA enVision facilita el cumplimiento de normas, ya que brinda informes “listos para usar” que muestran todos los cambios de configuración realizados en firewalls del grupo de dispositivos PCI. Informe: “PCI: Modificaciones en la Configuración del Firewall”</p>
<p>Requerimiento 1.1.9 Estándares de configuración para routers</p>	<p>Las plantillas de RSA enVision permiten a los clientes ver fácilmente todos los cambios de configuración realizados en routers del grupo de dispositivos PCI. Informe: “PCI: Modificaciones en la Configuración del Router”</p>

Reporting y Auditoría de PCI DSS y RSA enVision (continuación)

REQUERIMIENTOS DE PCI DSS

CAPACIDAD DE RSA enVISION

> Requerimiento 1.3

Generar una configuración del firewall que restrinja conexiones entre servidores accesibles públicamente y cualquier componente del sistema que almacene información de los titulares de tarjetas, incluso cualquier conexión desde redes inalámbricas. Esta configuración de firewall debe incluir lo siguiente:

<p>Requerimiento 1.3.1 Restringir el tráfico de Internet entrante a las direcciones de Protocolo de Internet (IP, <i>Internet Protocol</i>) dentro de la Zona Desmilitarizada (DMZ) (filtros Ingress).</p>	<p>Las capacidades de reporting de RSA enVision permiten a los clientes generar listas automáticas de todo el tráfico de Internet entrante en puertos no estándar del grupo de dispositivos PCI de manera detallada y resumida.</p> <p>Informe: "PCI: Tráfico de Internet Entrante en Puertos no Estándar, Detalle"</p>
<p>Requerimiento 1.3.2 No permitir que las direcciones internas pasen de Internet a la Zona Desmilitarizada (DMZ, <i>DeMilitarized Zone</i>).</p>	<p>RSA enVision proporciona plantillas integradas que permiten a los clientes simplificar el reporting de todo el tráfico de Internet entrante en puertos no estándar del grupo de dispositivos PCI de manera detallada y resumida.</p> <p>Informe: "PCI: Tráfico de Internet Entrante en Puertos no Estándar, Detalle"</p>
<p>Requerimiento 1.3.6 Asegurar y sincronizar los archivos de configuración de router. Por ejemplo, los archivos de configuración de ejecución (para el funcionamiento normal de los routers) y los archivos de configuración de inicio (cuando se reinician las máquinas) deben tener la misma configuración segura.</p>	<p>RSA enVision ofrece informes integrados que resumen todo el tráfico saliente por destino.</p> <p>Informe: "PCI: Resumen de Tráfico Saliente"</p> <p>Los informes de RSA enVision detallan todo el tráfico saliente de una dirección IP interna específica.</p> <p>Informe: "PCI: Detalle de Tráfico Saliente por Dirección de Origen"</p>
<p>Requerimiento 2.1.1 En los entornos inalámbricos, cambiar valores predeterminados de proveedores inalámbricos, como claves de red de privacidad equivalente por cable (WEP, <i>Wired Equivalent Privacy</i>), identificadores de conjuntos de servicios (SSID, <i>Service Set Identifier</i>) predeterminados, contraseñas y strings de la comunidad SNMP (Simple Network Management Protocol), entre otros. Desactivar difusión de SSID. Activar la tecnología de acceso WiFi protegido (WPA y WPA2) para encriptación y autenticación cuando exista capacidad WPA.</p>	<p>RSA enVision ofrece reporting integrado que detalla todos los cambios de configuración realizados en routers inalámbricos, lo que permite a los clientes demostrar fácilmente a un auditor que los valores predeterminados del proveedor, como claves WEP, SSID predeterminado, contraseña, strings de la comunidad SNMP y desactivación de transmisión de SSID, se modificaron antes de que se introdujera el router en el entorno de tarjetas de pago.</p> <p>Informe: "PCI: Modificaciones en la Configuración del Entorno Inalámbrico"</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.</p>	<p>RSA enVision ofrece informes integrados que permiten a los clientes detallar toda la generación y el cambio periódico de claves de encriptación utilizadas para procesos de almacenamiento de información seguro y transferencia de datos de las tarjetas de pago, al igual que resúmenes de detalles de control de acceso, como inicios de sesión exitosos o fallidos, aplicación de políticas y reporting regular.</p>
<p>> Requerimiento 4.1 Utilizar protocolos de seguridad y criptografía sólidos, 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>Las capacidades de reporting de RSA enVision permiten a los clientes acceder a todas las operaciones criptográficas en las que el uso de criptografía falló o fue desactivado por el usuario.</p> <p>Informe: "PCI: Fallas en Transmisiones Encriptadas"</p>

Reporting y Auditoría de PCI DSS y RSA enVision (continuación)

REQUERIMIENTOS DE PCI DSS	CAPACIDAD DE RSA enVISION
<p>> Requerimiento 5.2 Asegurarse de que todos los mecanismos antivirus estén actualizados, se ejecuten activamente y sean capaces de generar logs de auditoría.</p>	<p>RSA enVision ofrece plantillas de reporting que simplifican el trabajo de revisión de procedimientos de actualización de sistemas antivirus, tanto para administradores como para auditores.</p> <p>Informe: "PCI: Procedimientos de Actualización de Antivirus"</p>
<p>> Requerimiento 6.1 Asegurarse de que todos los componentes del sistema y el software tengan instaladas todas las correcciones de seguridad más recientes proporcionadas por los proveedores. Instalar las correcciones de seguridad correspondientes dentro del mes del lanzamiento.</p>	<p>RSA enVision ofrece informes integrados que proporcionan una vista de todas las correcciones y aplicaciones de service pack de sistemas basados en Microsoft Windows.</p> <p>Informe: "PCI: Aplicación de Correcciones Suministradas por Proveedores"</p>

RSA es su asociado de negocios de confianza

RSA, la División de Seguridad de EMC, cuenta con personal especializado en seguridad centrada en la información, lo que permite proteger la información a través de todo su ciclo de vida. RSA permite a los clientes asegurar de manera rentable los activos de información críticos y las identidades en línea (en el lugar y la etapa en que se encuentren) y administrar la información y los eventos de seguridad para aliviar la carga que impone el cumplimiento de normas.

RSA ofrece soluciones líderes en la industria de verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas e información de seguridad, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, visite www.RSA.com y www.EMC.com.

©2007 RSA Security Inc. Todos los derechos reservados.
RSA, 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 es una marca registrada de EMC Corporation. Todos los demás productos y servicios mencionados son marcas comerciales de sus respectivas empresas.

PCISIEM SB 0307



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

The Security Division of EMC