



Hoja de Datos del Producto

Cumplimiento Simplificado de Normas de TI:

La Plataforma RSA enVision®: Ayuda para Establecer Programas Rentables, Eficaces y Seguros de Cumplimiento de Normas Basados en Entornos

En Resumen

- Brinda control y visibilidad integrales y en tiempo real, en toda la empresa.
- Ayuda a satisfacer diferentes regulaciones de cumplimiento de normas desde un solo sistema.
- Soporta la creación de un entorno personalizado y proactivo de cumplimiento de normas de TI.
- Ofrece una amplia gama de informes que soportan cumplimiento de normas mundiales.

Cumplimiento de Normas más Eficaz de Diversas Regulaciones

Las empresas de todo el mundo deben enfrentar un aluvión de requerimientos de cumplimiento de normas provenientes de gobiernos, grupos industriales y políticas internas. Por lo general, la respuesta es reactiva cuando las empresas administran el cumplimiento de normas por proyecto. Como resultado, se suelen realizar implementaciones tecnológicas redundantes e invertir costos exorbitantes de TI relacionados con el cumplimiento de normas.

Existe una solución: estándares mundiales que brindan entornos de seguridad de TI para establecer el método más rentable y proactivo que permite administrar requerimientos de cumplimiento de normas y, de manera más general, riesgos de

información. Al basar las actividades de cumplimiento de normas de toda la empresa en estos estándares industriales, como ISO 27002, ITIL, CoBIT y COSO, puede mejorar considerablemente el cumplimiento de normas simultáneo de diferentes regulaciones, entre ellas, los requerimientos del Estándar de seguridad de datos de la industria de pagos con tarjeta (PCI DSS, *Payment Card Industry Data Security Standard*), HIPAA, Sarbanes-Oxley, sin necesidad de duplicar el esfuerzo ni la inversión y sin generar conflictos en políticas ni controles. Estos entornos también tienen el potencial para optimizar la seguridad general y la eficacia operativa al eliminar las deficiencias del programa de seguridad de TI de la organización.

Los Requerimientos Tecnológicos de un Entorno de Cumplimiento de Normas

Una de las principales razones para adoptar un entorno general de cumplimiento de normas es que, si se implementa correctamente, permite ver los riesgos que enfrentan la organización y su información confidencial, y consultar el estado del cumplimiento de normas.

Esta visibilidad depende de controles que brindan información completa, precisa y actualizada de los usuarios, activos, datos, procesos y políticas que participan en toda la infraestructura de TI. Y, dado que adopta un entorno de cumplimiento de normas para simplificar la carga de cumplimiento, deseará recopilar y administrar esta información de manera transparente y automatizada.

Eso es exactamente lo que ofrece la plataforma RSA enVision®. Está diseñada específicamente para soportar los principios que subyacen a los entornos de cumplimiento de normas como ISO 27002, entre otras, al simplificar el cumplimiento mediante la administración de riesgos para la información de toda la empresa.



The Security Division of EMC

¿En qué consiste la Plataforma RSA enVision?

La plataforma RSA enVision es una solución de administración todo en uno diseñada para simplificar el cumplimiento de normas, mejorar las operaciones de seguridad y optimizar las operaciones de redes y TI mediante la automatización de tareas de recopilación, análisis, alerta, auditoría, reporting y almacenamiento seguro de todos los logs. La recopilación de datos de logs de redes, archivos, aplicaciones y actividades de usuarios puede ayudarlo a probar su grado de cumplimiento de normas e identificar áreas de incumplimiento.

La plataforma RSA enVision ofrece muchas capacidades fundamentales para establecer un programa basado en entornos. Esta solución permite:

- Identificar automáticamente actividades de referencia, datos y activos de TI en toda la organización, lo que resulta fundamental para evaluar el riesgo eficazmente y formular planes de acción precisos.
- Intercalar, administrar y hacer archiving automático y seguro de logs de eventos obtenidos de todos los componentes de TI, incluso los administrados por terceros, para impulsar una mayor seguridad en toda la empresa.
- Monitorear continuamente los componentes de redes y los sistemas de información de negocios en busca de actividad e incidentes de seguridad y eventos para obtener los medios necesarios para cumplir las demandas de control de acceso y configuración, detección de malware, aplicación de políticas, administración y monitoreo de usuarios, y seguridad de transmisión y entorno.
- Emitir alertas a los administradores sobre incidentes de seguridad importantes en tiempo real, para permitir acciones correctivas inmediatas. La administración de incidentes constituye una parte crítica del cumplimiento eficaz de normas.

Simplificación del Reporting en Todo el Ecosistema de Cumplimiento de Normas

La plataforma RSA enVision también proporciona funcionalidades de reporting muy sofisticadas para simplificar el proceso de imposición permanente de cumplimiento de normas de los requerimientos regulatorios. Para cumplir las regulaciones que afectan al negocio y adaptarse a las políticas y al entorno de cumplimiento de normas específicos, los administradores pueden crear sus propios informes mediante una interfaz de asistente intuitiva. También puede aprovechar una serie de más de 1.100

plantillas de informes diseñadas para cubrir las principales regulaciones mundiales de cumplimiento de normas, entre ellas, SOX, HIPAA, PCI DSS, FISMA y SAS 70.

La plataforma RSA enVision incluye un elemento crucial para todo método de cumplimiento de entornos basado en estándares, es decir, una serie completa de informes listos para usar alineados directamente con secciones de la conocida norma ISO 27002. Esto significa que si adopta un entorno como ISO 27002 para administrar todos los requerimientos de cumplimiento de normas con mayor eficacia, contará inmediatamente con la mayoría de las funciones de reporting que necesita. Se incluyen más de 20 informes para ISO 27002, entre ellos:

- Control de datos de recursos humanos (sección 8.3)
- Informe de contratistas externos (secciones 8.1.3, 10.7.3)
- Actividad de software malicioso (sección 10.4.1)
- Cambio y vencimiento de contraseñas (sección 11.3.1)
- Actividad de usuarios desde dominios externos (sección 11.4.2)
- Actividad de inicio de sesión de cuentas de computadoras (sección 11.5.b)
- Estado de cuentas de computadoras por cuenta (sección 11.5.1)
- Informe de control de cambios de operaciones (sección 11.6)
- Control de software operacional (sección 12.4.1)
- Control de datos de prueba de sistemas (sección 12.4.2)
- Acceso a código fuente (sección 12.4.3)
- Control de evidencia recopilada (sección 13.2)
- Control de datos de auditorías de sistemas (sección 15.3.2)

La inteligencia que brinda la plataforma RSA enVision en estos informes permite acelerar el progreso hacia el establecimiento de un programa simplificado de cumplimiento de normas. El reporting de RSA enVision brinda la visibilidad necesaria para evaluar con más facilidad el inventario y los riesgos iniciales, implementar controles eficazmente y hacer seguimiento del progreso para generar mejoras continuas en el cumplimiento de normas.

Diseñado Específicamente para las Cláusulas ISO 27002

Al igual que las capacidades avanzadas de reporting, las funciones de inventario, referencia, análisis de tendencias, monitoreo y alerta de la plataforma RSA enVision ayudan a seguir muchas de las mejores prácticas especificadas de la norma ISO 27002 y brindan información útil para probar la eficacia de políticas y controles. En la siguiente tabla se detallan algunos puntos destacados.

Sección Mejores prácticas de ISO 27002 Contribución de la plataforma RSA enVision

Sección 10: Administración de comunicaciones y operaciones.

10.1.1	Documentación de procedimientos operativos	Monitorea, recopila y correlaciona logs de auditoría provenientes de más de 150 tipos de fuentes de eventos para establecer una referencia y brindar datos importantes para documentar los procedimientos operativos. Conserva información, es decir, IDs de usuarios, fechas y horarios de eventos clave, e intentos correctos y fallidos de acceder a recursos clave, entre otras opciones. Brinda administración automatizada del ciclo de vida para garantizar que los logs se conserven durante un período apropiado.
10.1.3	División de tareas y responsabilidades	Aplica la división de tareas al permitir que el personal acceda a logs de eventos para hacer su trabajo, sin otorgar acceso directo privilegiado a los sistemas de TI críticos encargados de generar los logs.
10.2.2	Monitoreo de actividades de terceros	Monitorea los sistemas de TI administrados por terceros para garantizar que todos los elementos se administren según establecen las normas.
10.3.1	Monitoreo de sistemas para prepararse para futuras necesidades de performance y capacidad	Correlaciona eventos de una amplia gama de componentes de la infraestructura para emitir alertas a los operadores sobre posibles problemas antes de que afecten a los usuarios, lo que permite que las organizaciones administren la capacidad del sistema con mayor eficacia.
10.6.1	Establecimiento de controles de seguridad de redes	Monitorea los componentes de red, como switches, firewalls, IDSs (Intrusion Detections Systems, <i>Sistemas de detección de intrusos</i>) y sistemas VPN, para emitir alertas inmediatas al personal de seguridad cuando se produce algún evento relacionado con la seguridad.
10.8.5	Protección de sistemas de TI del negocio	Monitorea los sistemas de información del negocio, proporciona visibilidad si se cumplen las normas y políticas de seguridad, y emite alertas a administradores sobre violaciones de políticas.
10.10.2	Monitoreo de uso del sistema	Monitorea y correlaciona eventos de sistemas de toda la infraestructura de manera continua. Además, emite alertas para notificar a los administradores cualquier actividad no autorizada.
10.10.3	Protección de logs de auditoría	Protege la evidencia de los logs al almacenar una gama de opciones seguras de almacenamiento de información de back-end.
10.10.4	Logs de actividad de usuarios avanzados	Recopila y monitorea todo tipo de log, incluso los logs de administradores de sistemas.
10.10.5	Revisión de logs con errores	Recopila todas las entradas de logs que se generaron con errores; emite alertas automáticas a los operadores cuando se produce un error.

Sección 12: Adquisición, desarrollo y mantenimiento de la seguridad de la información. Cómo utilizar técnicas para impedir la filtración de datos confidenciales.

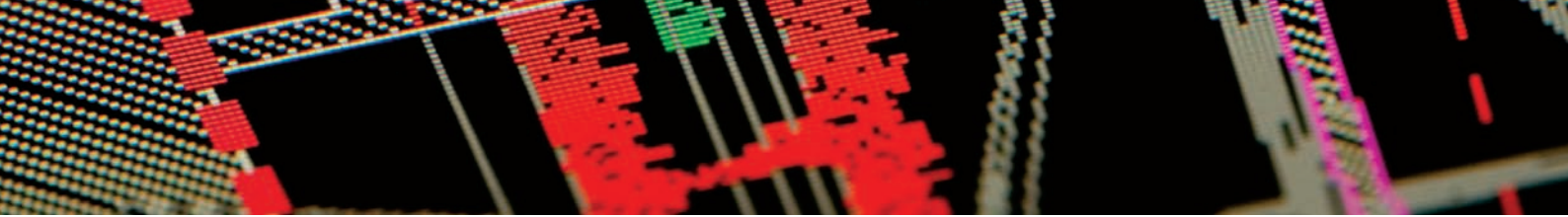
12.5.1	Establecimiento de procedimientos formales de control de cambios	Monitorea el entorno y los informes sobre todos los cambios en busca de una correlación con un proceso de cambio aprobado.
--------	--	--

Sección 13: Administración de incidentes de seguridad de la información.

13.1.1	Informe instantáneo de eventos de seguridad	Detecta posibles eventos de seguridad y notifica a los administradores en tiempo real.
13.2.2	Monitoreo y medición del impacto de incidentes de seguridad	Monitorea eficazmente los tipos de incidentes de seguridad que se producen y emite informes al respecto para ayudar al negocio a cuantificar el impacto de las amenazas de seguridad.
13.2.3	Conservación de evidencia relacionada con eventos de seguridad	Ofrece una base de datos con motor de búsqueda de todos los logs de eventos recopilados para simplificar el descubrimiento de todos los eventos relacionados con un incidente de seguridad específico.

Sección 15: Cumplimiento de normas. Cómo satisfacer los requerimientos internos y externos de cumplimiento de normas.

15.2.2	Revisión del cumplimiento de normas de seguridad técnica	Monitorea continuamente los eventos del entorno de TI para detectar y emitir informes de manera automática sobre todas las actividades que no cumplen las normas.
15.3.2	Protección de herramientas de auditoría de sistemas de información	Crea muchos controles de acceso, lo que brinda a los usuarios el acceso necesario a la información de los logs de eventos sin brindar acceso directo a los propios logs.



Acerca de RSA

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad para aceleración del negocio y ayuda a las más importantes organizaciones del mundo a alcanzar el éxito resolviendo los más complejos y delicados desafíos de seguridad. El enfoque hacia la seguridad centrado en la información que ofrece RSA protege la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar dónde se la mueva, quién acceda a ella o cómo se la use.

RSA ofrece soluciones líderes en verificación de la identidad y control de acceso, prevención de pérdida de datos y encriptación, administración de información de seguridad y cumplimiento de normas, 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 argentina.rsa.com y argentina.emc.com.

Más información

Para obtener más información sobre el método de cumplimiento de normas de RSA basado en entornos, visite <http://argentina.rsa.com/node.aspx?id=2763>, donde encontrará lo siguiente:

- Una visión general del método de entornos basado en estándares.
- Un informe de las soluciones donde se detalla cómo RSA puede ayudarlo a implementar un entorno ideal para su organización.
- Una hoja de datos de servicios que detalla las opciones de soporte que ofrece RSA y nuestro proceso de cinco pasos para implementar un entorno.
- Una hoja de datos del producto que detalla la gama completa de soluciones que complementan la plataforma RSA enVision en la implementación de un entorno de cumplimiento de normas.



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

The Security Division of EMC

RSA, el logotipo de RSA y enVision son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca comercial de EMC Corporation. Todas las otras marcas comerciales que aparecen aquí son propiedad de sus respectivos dueños.