

# Servicio de análisis y diseño de operaciones de seguridad

## Desarrollo de la funcionalidad de operaciones de seguridad

### En resumen

- Establece un plan de implementación o mejora de procedimientos y funcionalidades de operaciones de seguridad que incluyen dominios técnicos, operativos y del negocio.
- Proporciona un diseño general, centrado en SIEM y DLP, y un marco de trabajo de manejo de incidentes.
- Están basados en mejores prácticas y estándares y metodologías de implementación comprobados, por ejemplo, ISO, SANS y NIST.
- Aprovecha la experiencia de RSA con clientes del mundo real y el equipo global de respuesta a incidentes críticos de EMC.

Actualmente, las empresas enfrentan retos opuestos, ya que deben proteger las operaciones y la información contra riesgos. Por un lado, se observa un crecimiento de la cantidad de amenazas y de la sofisticación de los ataques. Por otro lado, es necesario tener en cuenta la realidad económica actual: los presupuestos se reducen, los recursos son limitados y los costos de administración de incidentes de seguridad son más elevados que antes.

Una función de operaciones de seguridad avanzada se centra en procesos que, a diario, permiten a las organizaciones proteger los recursos críticos de manera más eficiente y garantizar el cumplimiento de normas por medio de actividades de detección de incidentes, respuesta y resolución de problemas clave. En especial:

- Identificación y desarrollo cuidadosamente considerados de un programa integral de operaciones de seguridad.
- Diseño eficiente de un sistema de operaciones de seguridad que se centre en el uso integrado de sistemas y tecnologías de inteligencia de amenazas, SIEM y DLP.
- Integración con tecnologías de operaciones de red y administración de servicios, por ejemplo, centro de servicios, administración de configuraciones y cambios, y marcos de trabajo operativos como ITIL.

- Creación de un marco de trabajo sostenible para la administración de riesgos de información y seguridad a largo plazo.

Con la función de operaciones de seguridad avanzadas establecida, las organizaciones podrán implementar los procesos y las funcionalidades que necesitan para iniciar eficientemente un programa integral de administración de riesgos de la información.

### Análisis y diseño de operaciones de seguridad

Este servicio de consultoría y asesoramiento proporciona un amplio análisis de los requisitos de las operaciones de seguridad y las funcionalidades del estado actual, y recomienda un diseño de solución para cumplir con los objetivos específicos de administración de incidentes y operaciones de seguridad. También incluye un marco de trabajo para la administración de incidentes y los pasos a seguir para el desarrollo de políticas y procedimientos operativos y de administración adecuados. El servicio Análisis y diseño de operaciones de seguridad puede establecer la base para operaciones de seguridad avanzadas, además de ser el primer paso hacia un programa de operaciones de seguridad más avanzadas o un conjunto de funcionalidades del centro de operaciones de seguridad (SOC).

Basada en el análisis del negocio y los requisitos operativos y técnicos para funcionalidades de prevención de pérdida de datos y manejo general de incidentes, esta contratación incluye cuatro componentes principales:

- Análisis de alto nivel de los requisitos del negocio para soportar una función de operaciones de seguridad.
- Análisis detallado de los requisitos operativos y técnicos para soportar una función de operaciones de seguridad, en particular los requisitos de administración de eventos e información de seguridad (SIEM) y prevención de pérdida de datos (DLP) como principales tecnologías de seguridad del SOC.
- Arquitecturas de referencia para la plataforma RSA enVision® y las soluciones RSA® Data Loss Prevention para cumplir con los requisitos establecidos.
- Marco de trabajo de manejo de incidentes y próximos pasos para una planificación de operaciones y un diseño de solución más completos.





**Marco de trabajo de operaciones de seguridad**

RSA Professional Services ofrece una serie de servicios de consultoría y asesoramiento destinada a satisfacer los requisitos de las empresas que desean desarrollar su función de operaciones de seguridad.

**Alcance y enfoque**

El aumento de la sofisticación de los ataques de los hackers y los riesgos generados por el personal interno hacen que las organizaciones tomen una postura más dinámica para enfrentar la exposición a los riesgos de la información. Esto pone a prueba los métodos tradicionales de las operaciones de seguridad, que se limitan principalmente a la recopilación y el análisis de eventos de seguridad, y amplía el alcance de las operaciones de seguridad. Actualmente, una funcionalidad avanzada debe incluir el monitoreo y la protección de información confidencial y de la infraestructura en la que esta se encuentre o por la que se pueda transferir, además de poder monitorear y crear informes sobre los riesgos de seguridad de la información desde diversos orígenes en toda la empresa.

En respuesta a esta necesidad, RSA Professional Services desarrolló el servicio Análisis y diseño de operaciones de seguridad, que amplía su alcance para incluir cada uno de los aspectos de desarrollo de la función de operaciones de seguridad de un Cliente, es decir, desde la recopilación y el análisis de requisitos hasta el diseño adecuado de una solución, un plan de trabajo y un marco de trabajo de respuesta a incidentes.

El alcance y el enfoque para brindar este servicio incluyen las siguientes cuatro fases:

**Fase 1: estrategia de la solución**

- Estrategia de descripción inicial pre-site, objetivos y planificación de la contratación.
- Taller en sitio basado en el análisis de los requisitos de las operaciones de seguridad en función de las necesidades operativas, técnicas y del negocio.
- Identificación de orígenes de eventos y datos para monitoreo.
- Recorrido del proceso de manejo de incidentes.

**Fase 2: diseño de la solución**

- Desarrollo del diseño de la solución técnica en función de los requisitos.
- Identificación de orígenes de eventos de seguridad, requisitos de protección de datos, configuración, volúmenes de eventos y performance, y requisitos de almacenamiento.
- Desarrollo de configuraciones de soluciones SIEM y DLP apropiadas.

**Fase 3: revisión preliminar de la solución**

**Informe de análisis y diseño**

**Fase 4: informe final y presentación**