

# [NEG] Security Operations Center

Las principales funciones de un SOC son las siguientes:

- Monitorización y gestión de todos los activos de la empresa en tiempo real
- Securitización y fortificación de activos
- Respuesta ante amenazas proactiva y reactiva
- Toma de decisiones frente a incidentes
- Recuperación y mantenimiento del negocio
- Evaluación del riesgo y cumplimiento normativo.
- Evaluación del riesgo y cumplimiento normativo
- Reporting y procesos de mejora.

Para poder implementar un SOC es necesaria la transferencia de conocimiento, estrategia, procesos y políticas de la organización, conocimiento de los sistemas y dispositivos y una cadena de mando y comunicación. El problema es que es muy costoso. Un SOC puede ser implementado de varias maneras:

- On-Premise
- Hybrid
- Outsourcing

## Fases de la implementación de un SOC On-Premise

1. Tecnología: Personal encargado de analizar la organización para ver que herramientas son necesarias para poder obtener datos para el SOC
2. Securitización: Securitizar los equipos y documentarlos.
3. Políticas: Revisar políticas de seguridad de la empresa. Se recomienda basarlas en la ISO 27002.
4. Operación: Monitorización y testeo de equipos, respuesta a incidentes.... Permite conocer el funcionamiento de la organización y aplicar los cambios previstos en la política de seguridad
5. Inteligencia: Uso de herramientas de inteligencia que pueden anticipar problemas proactivamente.

## Inputs de un SOC

- Eventos: Observaciones registrables. Puede generarse un log u otra fuente de entradas con eventos
  - Muchos eventos pueden ser configurados para emitir una alerta. Esto se hace para eventos de interés que deben ser vigilados y pueden requerir intervención. Se suelen configurar en la herramienta SIEM
  - Las alertas generan incidentes que deben ser registrados a través de herramientas de ticketing o Service Desk.
- Problemas: Uno o más incidentes que no tienen una causa raíz identificada.
  - La gestión de problemas se ocupa de investigar y solucionar la causa raíz de los incidentes y encontrar soluciones permanentes y así intervenirlos en el futuro.

## Infraestructura de un SOC

- Infraestructura de seguridad en la organización: Dispositivos que permiten mantener confidencialidad, disponibilidad e integridad.
  - NAC: Network Access Control
  - DLP: Data Loss Prevention
  - IDS: Intrusion Detection System
- Infraestructura de seguridad en el SOC: Dispositivos y herramientas para revisar y analizar la información recibida en el SOC.
  - SIEM: Sistemas de gestión de eventos de seguridad (Security Information and Event Management)
  - Ticketing: Sistemas de gestión de incidencias
  - Herramientas de ayuda instaladas en equipos específicos (Honeypots)

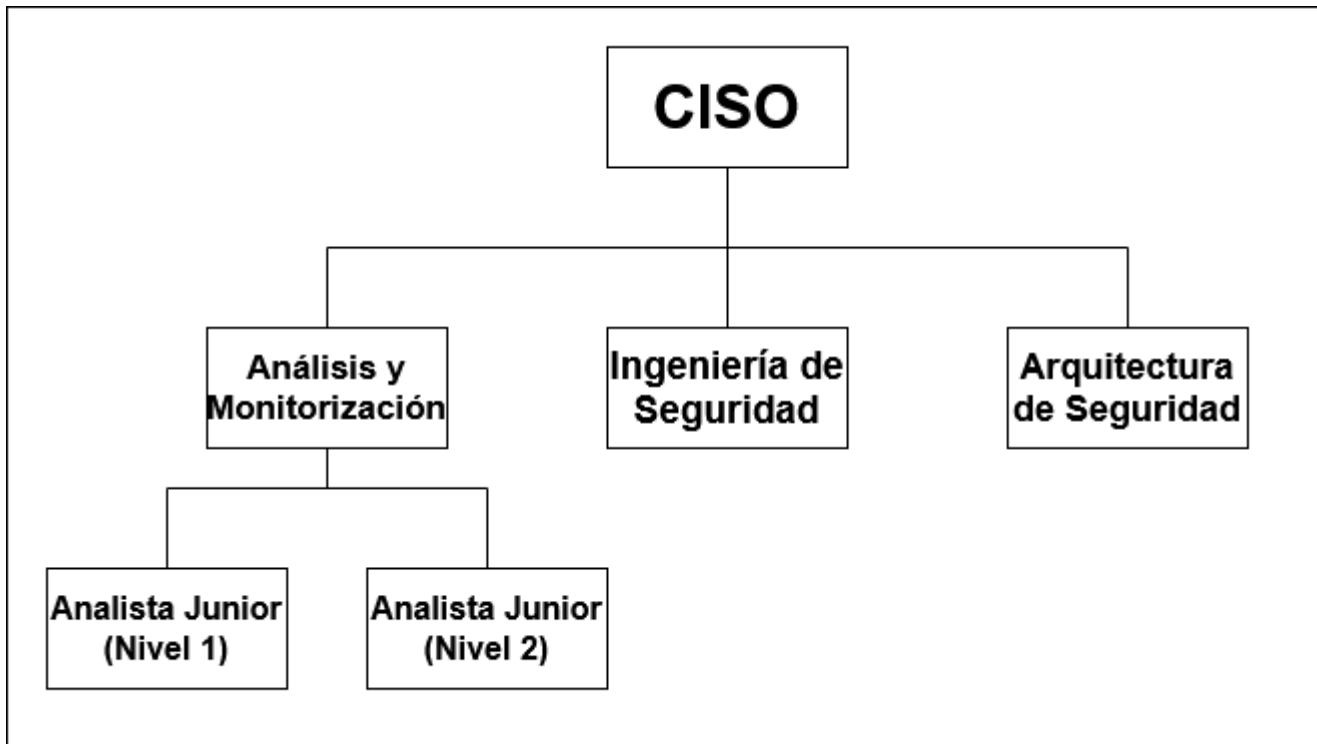
Las principales fuentes de datos suelen ser los logs y el SIEM

- Logs: Permiten realizar un triage y diagnóstico de amenazas y anomalías como errores de hardware, servicios anómalos, fallos de autenticación, registro de tareas de administración... Los aspectos importantes del log son los siguientes:
  - Monitorizar el log para garantizar su correcto funcionamiento
  - Revisar el almacenamiento y rendimiento
  - Sincronización con NTP para el registro cronológico.
  - Proteger la información que no debe aparecer en un log (contraseñas, información personal...)
  - La información debe clasificarse en niveles de severidad para su filtrado.
  - Los logs se pueden utilizar para detectar fraudes, realizar análisis forense y para auditorías
- SIEM: Puede llevar a cabo tareas y detecciones más complejas derivadas de los procesos de correlación e inteligencia.

## Ticketing Systems

Sin herramientas que consisten en una base de datos de activos y una base de conocimiento con información sobre los verdaderos positivos en contraparte a los falsos positivos en relación a los tickets relacionados. Los tickets son puntuados y clasificados (Triage). El sistema de ticketing permite diseñar el proceso a seguir y los pasos del workflow de resolución que pueden ser vitales para reducir el impacto y tiempo.

## Estructura Organizativa de un SOC



Es importante que tenga capacidad para influir en las decisiones de la organización que permitan mitigar y recuperar de forma óptima la actividad de una organización. Es muy importante la velocidad de respuesta y toma de decisiones.

## CIO-CISO

- El director de sistemas informáticos (CIO: Chief IT Officer) es el principal responsable del departamento IT y muchas veces, del SOC. Sus decisiones y planes añaden amenazas de seguridad y pueden introducir grandes riesgos en la organización. Muchas veces tiene prioridad la reducción de costes y tiempo frente a la seguridad.
- El director de seguridad de la información (CISO: Chief Information Security Officer) es el máximo responsable de la seguridad y del SOC. Responsable de las decisiones de seguridad corporativa, cumplimiento normativo y continuidad de negocio.

## Analista de Seguridad

- Forma parte de la primera línea de seguridad
- Responde a las fuentes de datos
- revisa eventos y alertas, realizando el primer triage.
- suelen tener 2 niveles:
  - Primer Nivel: Encargados de abrir los tickets y analizar que está ocurriendo, siguiendo un procedimiento estricto
  - Segundo Nivel o Senior: Encargado de tratar con los tickets escalados que necesitan análisis más detallado y experimentado.

## Ingenieros de Seguridad

Especializados en necesidades específicas de la organización como IDS, Proxy, Data Loss Prevention, etc...

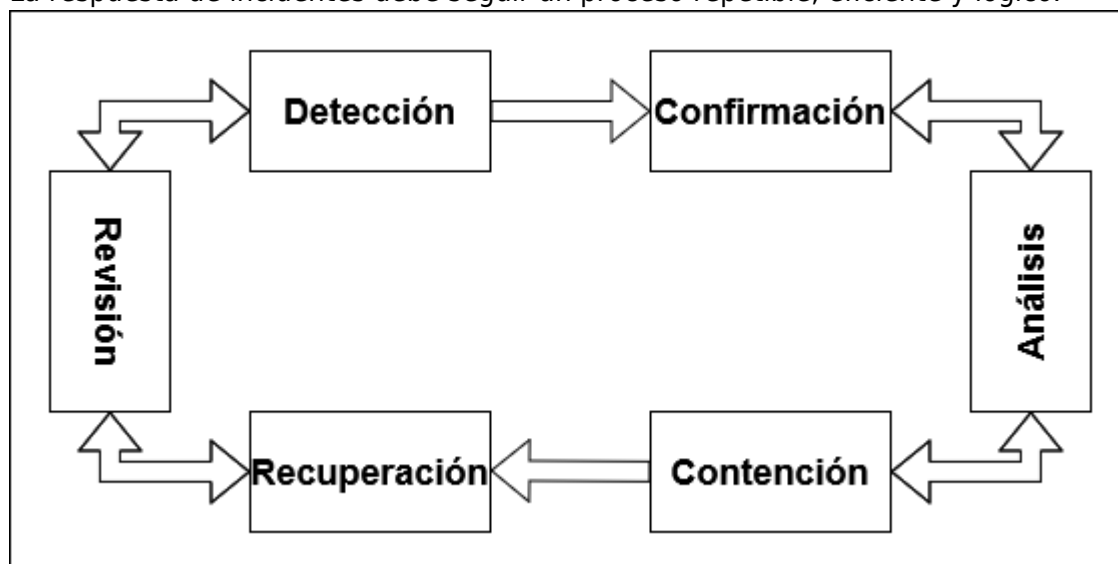
- Encargados de crear reglas en el SIEM y sistemas de alertas. Ajustan estas reglas para evitar falsos positivos
- Revisión de tickets cerrados por parte de los analistas para verificar su calidad y mejorar el proceso
- Formar a los analistas para favorecer el triage y cierre de casos normales.

## Arquitectos de seguridad

Realizan la determinación de requerimientos, planificación y seguimiento de los sistemas de seguridad para alcanzar los objetivos organizacionales. Se aseguran de que las incorporaciones de nuevas tecnologías sean bien gestionadas por el SOC y que se integran correctamente con las herramientas del SOC. Es responsable del análisis de riesgos, pruebas de vulnerabilidad, evaluaciones de seguridad e implantación de arquitecturas y plataformas de seguridad.

## Operación de un SOC

La respuesta de incidentes debe seguir un proceso repetible, eficiente y lógico.



## Métricas

Las métricas sobre el día a día del SOC facilitan información sobre posibles problemas

- Métricas sobre cumplimiento de objetivos
- Estado de los tickets de alta prioridad
- Duración de la resolución de un determinado tipo de tickets

## Clasificación de vulnerabilidades

Se clasifican de varias formas:

- Forma simple

- Bajo (Niveles 1 al 4)
- Medio (Niveles 4.1 al 7)
- Alto (Niveles 7.1 al 10)
- PCI
  - Nivel 1 al 5
- Severidad
  - Bajo
  - Importante
  - Medio
  - Severo
  - Crítico
- CVSS: Sistema de clasificación público. La NVD (National Vulnerability Database) toene un repo de vilnerabilidades con este tipo de puntuación
  - Del 0 al 10

## Clasificación de activos

Es necesario clasificar todos los activos de la organización para dar una respuesta eficaz en caso de ataques y saber cuales priorizar en función a ciertos criterios marcados. Se debe llevar un control de las estadísticas de los activos que van a marcar las eficiencia de las contramedidas. La clasificación se realiza por:

- Impacto en el negocio
- Impacto financiero de la caída de un servicio
- Requisitos de alta disponibilidad
- Impacto en la seguridad
- Tiempo medio entre fallos y probabilidades de fallo
- Valor de reemplazo
- Número de usuarios
- Almacenamiento de información crítica
- Impacto reputacional

## Histórico de parches

Se debe monitorizar el historial de parches para saber cuales no se han aplicado en activos críticos. En función a esto se pueden determinar vilnerabilidades abietas en función a los parches aplicados. El tiempo medio de aplicación de parches mide la ventana de oportunidad para las vulnerabilidades involucradas.

## Inteligencia

Se basa en el análisis de una gran colección de información externa e interna. El SOC puede tomar las siguientes decisiones de protección:

- Limitar el espacio de IPs
- Incorporar listas de osp desde las qe se hace spam
- usar colecciones de info acercade ataques para detectar comportamientos anómalos.

## Blacklist

- Facilitan el reconocimiento de orígenes problemáticos en cuanto a spam, malware, etc...
- Se pueden incluir URIs que contienen orígenes de ataques phishing, pharming, etc...
- Se pueden analizar patrones y contenido de los email para detectar ataques que han modificado sus direcciones para no ser detectados por la blacklist

## Bases de datos externas

Organizaciones y fabricantes comparten información sobre ataques y amenazas para informar a sus clientes y promocionar sus productos.:

- atlas.arbor.net: Recursos sobre vulnerabilidades detectadas por Netscout
- SecurityFocus.com: Vulnerabilidades localizadas por Symantec
- SenderBase.org: Reputación de tráfico de email de acuerdo a Cisco
- SpamHaus.org: Base de datos en tiempo real con direcciones IP de equipos secuestrados por exploits y lista de email o reputación de dominio.

## Organizaciones y Partners Industriales

- Se paga por información de seguridad para tener un conocimiento más exacto de ciertos tipos y grupos de ataques.
- Advanced Persistent Thread (APT): Ataques muy sofisticados y persistentes en el tiempo que se pueden usar para espionaje, sabotaje de cadenas de suministro, ingeniería social...
- Interesa participar en organizaciones que comparten recursos comunes e información sobre seguridad como las ISAC (Information Sharing and Analysis Center).

## Outsourcing del SOC

### MSSP (Managed Security Services Provider)

- Primero se define el tipo de operaciones que se van a externalizar y que estas no se solapan con las internas.
- Los MSS (Managed Security Services) pueden tener varias prestaciones:
  - Analistas de seguridad
  - Ingenieros especialistas en seguridad para IDS
  - Gestión remota del perímetro
  - Respuesta a incidentes
  - Gestión de vulnerabilidades y parches
- Existen varios tipos de MSSP en función de la estrategia, situación financiera y tolerancia al riesgo:
  - Strategic Partners: Tienen experiencia previa y relación con el mundo IT. La seguridad puede no ser su punto fuerte o no disponer de lo que se necesita
  - Pure Play Providers: Dedicados al negocio de seguridad, tienen formación competente y su precio es elevado en consecuencia.
  - Boutique Providers: Pequeños MSSP orientados a un área específica de seguridad.

## Ventajas de los MSSP

- Están preparados para tratar con muchos tipos de eventos, el personal está entrenado y formado para dar una respuesta rápida en situaciones estresantes y cuentan con gran experiencia en la gestión de eventos de seguridad de forma efectiva y eficiente. Muchas veces tienen especialización vertical.
- El coste suele ser menor que tener un SOC propio.
- Supresión de los reinos de taifas en la monitorización y gestión del equipamiento. Coordinación de diversos departamentos.
- SLA (Service Level Agreement): Los MSSP trabajan en función del nivel y tipo de servicio.
- Documentación: Los procedimientos de un MSSP suelen estar bien documentados, con políticas bien definidas y los procesos internos bien documentados.

## Desventajas de los MSSP

- Si un MSSP tiene demasiados clientes, dificulta en conocimiento de cada uno de ellos
- Falta de recursos dedicados, si hay crisis con múltiples empresas de diferentes sectores a la vez puede no haber suficientes recursos para atender a todos los clientes.
- Problemas de almacenamiento de datos: la capacidad, privacidad, regulaciones y persistencia de datos

## Requisitos para el Outsourcing del SOC

- Indagar que recursos es necesario involucrar
- Asegurar la certificación y formación del personal que suministra el servicio
- Asegurar que cuenten con un balanceo entre tamaño y experiencia adecuado.
- Definir como se aplicará el servicio, cuales serán los canales de comunicación y que se deberá comunicar
- Que herramientas y sistemas de información o autoservicio estará a disposición del cliente.

## Prestación de servicios

- Disaster Recovery y plan que se ejecutará en los diferentes escenarios que ocurran
- Estrategia de salida: Como será el fin del contrato.

From:

<http://www.knoppia.net/> - **Knoppia**

Permanent link:

[http://www.knoppia.net/doku.php?id=master\\_cs:negocio:tm1](http://www.knoppia.net/doku.php?id=master_cs:negocio:tm1)

Last update: **2025/02/27 13:16**

