**Roles en respuesta**

Hasta ahora, has obtenido información sobre el **ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST)**, que es un marco de trabajo para la respuesta a incidentes que consta de cuatro fases:

* Preparación.
* Detección y análisis.
* Contención, erradicación y recuperación.
* Actividad posterior a un incidente.

Como profesional de la seguridad, trabajarás en equipo para monitorear, detectar y responder a incidentes. Antes, aprendiste sobre **equipos de respuesta a incidentes de seguridad informática (CSIRT)** y un **Centro de Operaciones de Seguridad (SOC)**. En esta lectura ampliarás tus conocimientos acerca de las diferentes funciones, roles y responsabilidades que conforman los CSIRT y los SOC.

Comprender la composición de los equipos de respuesta a incidentes te facilitará la navegación dentro de la jerarquía de una organización, al permitirte colaborar y comunicarte de manera efectiva con otros miembros del equipo, y trabajar de forma cohesionada en la respuesta a incidentes. ¡Incluso, podrías descubrir roles específicos que despierten tu interés mientras comienzas tu carrera en seguridad!

**Mando, control y comunicación**

Un **equipo de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés)** es un grupo de personas especializadas en seguridad, capacitadas en gestión y respuesta a incidentes. Durante la respuesta a incidentes, los equipos pueden enfrentar diversos desafíos. Para que la respuesta a incidentes sea efectiva y eficiente, es necesario contar con un mando claro**,** control y comunicación de la situación, a fin de lograr el objetivo deseado.

* **El mando** se refiere a tener el liderazgo adecuado y la dirección necesaria para supervisar la respuesta.
* **El control** se refiere a la capacidad de gestionar los aspectos técnicos durante la respuesta a incidentes, como coordinar recursos y asignar tareas.
* **La comunicación** se refiere a la capacidad de mantener informadas a las partes interesadas.

Establecer una estructura organizativa CSIRT con funciones claras y diferenciadas ayuda a alcanzar una respuesta efectiva y eficiente.

**Roles en un CSIRT**

Los equipos de respuesta a incidentes de seguridad informática (CSIRT) dependen de la organización, lo que significa que pueden variar en cuanto a su estructura y funcionamiento. Desde una perspectiva estructural, pueden existir como un equipo independiente y dedicado o como un grupo de trabajo que se reúne cuando es necesario. Los CSIRTs involucran tanto a profesionales especializados en la seguridad como a profesionales no especializados. Con frecuencia se consulta a profesionales no especializados en seguridad para que brinden su experiencia en relación con el incidente. Estos profesionales pueden provenir de departamentos externos, como recursos humanos, relaciones públicas, administración, TI, legales y otros. Los profesionales de seguridad que forman parte de un CSIRT suelen desempeñar tres funciones clave relacionadas con la seguridad:

1. **Analista de seguridad**
2. **Responsable técnico**
3. **Coordinador de incidentes**

**Analista de seguridad**

El trabajo del **analista de** **seguridad** consiste en monitorear de manera continua un entorno en busca de posibles amenazas a la seguridad. Esto incluye:

* Analizar y clasificar las alertas.
* Realizar investigaciones de causa raíz.
* Notificar a superiores o resolver las alertas.

Si se identifica una amenaza crítica, los analistas la remiten al líder correspondiente del equipo, como el responsable técnico.

**Responsable técnico**

El trabajo del responsable técnico es gestionar todos los aspectos técnicos del proceso de respuesta a incidentes, como la aplicación de parches o actualizaciones de software. Para ello, primero determina la causa raíz del incidente. Luego, crea e implementa las estrategias para contener, erradicar y recuperarse del incidente. Los responsables técnicos suelen colaborar con otros equipos para asegurarse de que sus prioridades en la respuesta a incidentes se alineen con las prioridades del negocio, como la reducción de interrupciones para los clientes o el retorno a la normalidad de las operaciones.

**Coordinador de incidentes**

La respuesta a un incidente también implica una colaboración interdisciplinaria con profesionales que no se especializan en seguridad. Los equipos de respuesta a incidentes de seguridad informática (CSIRT) suelen consultar y aprovechar la experiencia de miembros de departamentos externos. La persona a cargo de la coordinación de incidentes tiene la función de coordinar la tarea con los departamentos pertinentes durante un incidente de seguridad. Al hacerlo, se mantienen abiertas y claras las líneas de comunicación, y queda informado a todo el personal sobre el estado del incidente. Los coordinadores de incidentes también pueden encontrarse en otros equipos, como el Centro de Operaciones de Seguridad (SOC).

**Otros roles**

Dependiendo de la organización, se pueden encontrar muchos otros roles en un equipo de respuesta a incidentes de seguridad informática (CSIRT), incluyendo responsables de comunicación, de legales o de planificación, entre otros.

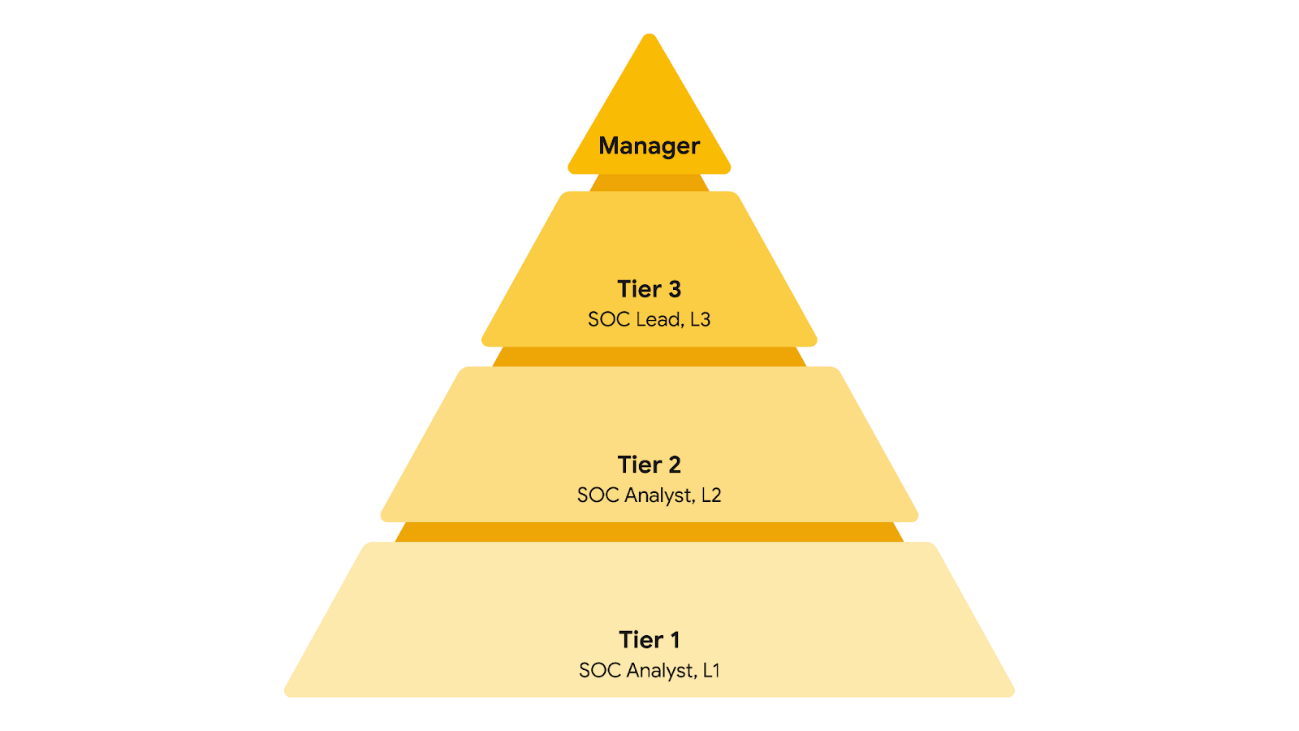
**Nota**: Los equipos, roles, responsabilidades y estructuras organizativas pueden variar en cada empresa. Por ejemplo, algunas funciones diferentes para la persona a cargo de la coordinación de incidentes incluyen la dirección y gerencia de incidentes.

**Centro de Operaciones de Seguridad**

Un **Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés)** es una unidad organizativa dedicada a monitorear redes, sistemas y dispositivos en busca de amenazas o ataques de seguridad. Estructuralmente, un SOC suele existir como unidad independiente o dentro de un CSIRT. Es posible que te hayas familiarizado con el término *equipo azul*, que se refiere a los profesionales de seguridad responsables de la defensa contra todas las amenazas y ataques a la seguridad en una organización. Un SOC participa en diversas actividades del equipo azul, como el monitoreo de redes, el análisis y la respuesta a incidentes.

**Organización de un SOC**

Un Centro de Operaciones de Seguridad (SOC) está compuesto por analistas, líderes y gerentes. Cada función tiene sus propias responsabilidades. Los analistas SOC se agrupan en tres niveles diferentes.



**Analista SOC de nivel 1**

El primer nivel está compuesto por los analistas SOC menos experimentados, conocidos como analistas de nivel 1 (L1, por level 1). Son responsables de:

* Monitorear, revisar y priorizar las alertas basándose en su criticidad o gravedad.
* Crear y cerrar alertas utilizando sistemas de tickets.
* Notificar los tickets de alerta a los niveles 2 o 3.

**Analista SOC de nivel 2**

El segundo nivel está formado por los analistas SOC más experimentados, o analistas de nivel 2 (L2). Son responsables de:

* Recibir tickets escalados de L1 y realizar investigaciones más profundas.
* Configurar y perfeccionar las herramientas de seguridad.
* Reportar al líder SOC.

**Líder SOC de nivel 3**

El tercer nivel de un SOC está compuesto por los jefes SOC o líderes de nivel 3 (L3s). Estos profesionales altamente experimentados son responsables de:

* Gestionar las operaciones de su equipo.
* Explorar métodos de detección mediante la realización de técnicas de detección avanzadas, como el análisis forense y de malware.
* Reportar al gerente SOC

**Gerente SOC**

El gerente SOC está en la parte superior de la pirámide y es responsable de:

* Contratar, formar y evaluar a los miembros del equipo SOC.
* Crear métricas y gestionar el rendimiento del equipo SOC.
* Desarrollar informes relacionados con incidentes, cumplimiento normativo y auditoría.
* Comunicar los resultados a las partes interesadas, como la dirección ejecutiva.

**Otros roles**

Los SOC también pueden contener otras funciones especializadas, como ser:

* **Investigadores forenses**: pertenecen comúnmente a L2 y L3, y recopilan, conservan y analizan pruebas digitales relacionadas con incidentes de seguridad para determinar lo sucedido.
* **Cazadores de amenazas**: suelen ser L3 que trabajan para detectar, analizar y defenderse contra amenazas de ciberseguridad nuevas y avanzadas, utilizando inteligencia de amenazas.

**Nota**: Al igual que los CSIRT, la estructura organizativa de un SOC puede variar dependiendo de la organización.

**Conclusiones clave**

Como analista de seguridad, trabajarás en colaboración con los miembros de tu equipo y con personas ajenas a él. Comprender la estructura organizativa de un equipo de respuesta a incidentes, ya sea un CSIRT o un SOC, te permitirá entender cómo los incidentes avanzan a lo largo de su ciclo de vida y las responsabilidades de los diversos roles de seguridad a lo largo de todo el proceso. Tener claridad sobre tu rol y el de otros profesionales durante un evento de respuesta a incidentes te facilitará enfrentar situaciones de seguridad desafiantes al aprovechar diferentes perspectivas y buscar soluciones creativas.

**Recursos para obtener información adicional**

Aquí tienes algunos recursos si deseas obtener más información sobre la organización de un SOC o explorar otras funciones de respuesta a incidentes:

* [El ecosistema de operaciones de seguridad.](https://chronicle.security/blog/posts/soc-ecosystem-infographic/)
* [Herramienta de trayectorias profesionales en ciberseguridad.](https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool)
* [Detección y respuesta](https://www.youtube.com/watch?v=QZ0cpBocl3c) en Google: Episodio 2 de la serie de videos de [Hackeo a Google](https://www.youtube.com/playlist?list=PL590L5WQmH8dsxxz7ooJAgmijwOz0lh2H).