LIBRO BLANCO DEL SOC

en colaboración con:

isms forum

CSC
CYBER SECURITY CENTRE

Red Nacional de SOC

COORDINADORES

ALEJANDRO ALIAGA

JAVIER SEVILLANO

PARTICIPANTES

ALEJANDRO AGUDELO

ANÍBAL DÍAZ

ARTURO BELTRÁN

CARLOS ANTONINI CEPEDA

DAVID ALCARAZ

DAVID DE LA ROSA

EDWIN BLOM

ENRIC ALIBECH

ETXAHUN SÁNCHEZ

HIRAM FERNÁNDEZ

JAVIER DÍAZ

JOSE LUIS GALLEGO

JOSE LUIS JIMÉNEZ

JOSE RAMÓN CONCHA

OLIVER LÓPEZ

JUAN CARLOS AGÜERO

JUANAN ALCARAZ

MAIT SAGARRA

MARA FERNÁNDEZ

MARÍA RAMÍREZ

MIGUEL JIMÉNEZ

ÓSCAR LÓPEZ

RAFAEL VIDAL

SANTIAGO BAYO

SERAFÍ VICENT

SERGIO BILBAO

GESTIÓN DEL PROYECTO

BEATRIZ GARCÍA

SUSANA MARÍN

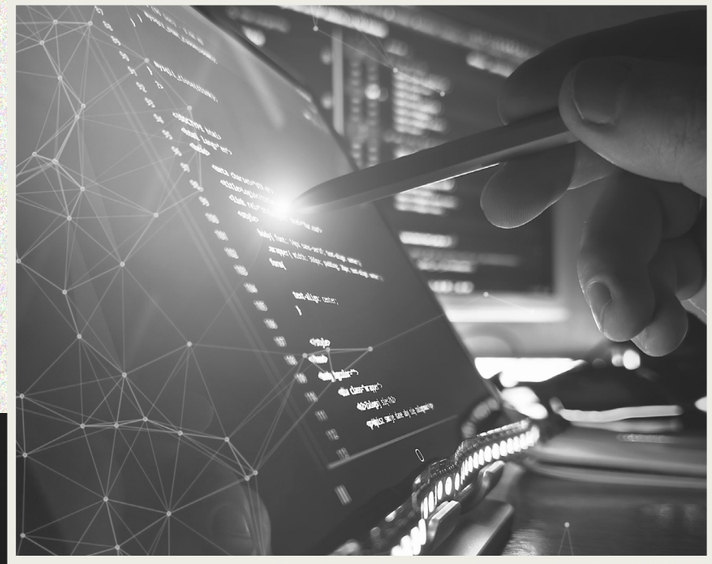
DISEÑO Y MAQUETACIÓN

SUSANA MARÍN

ÍNDICE

INTRODUCCIÓN

1.

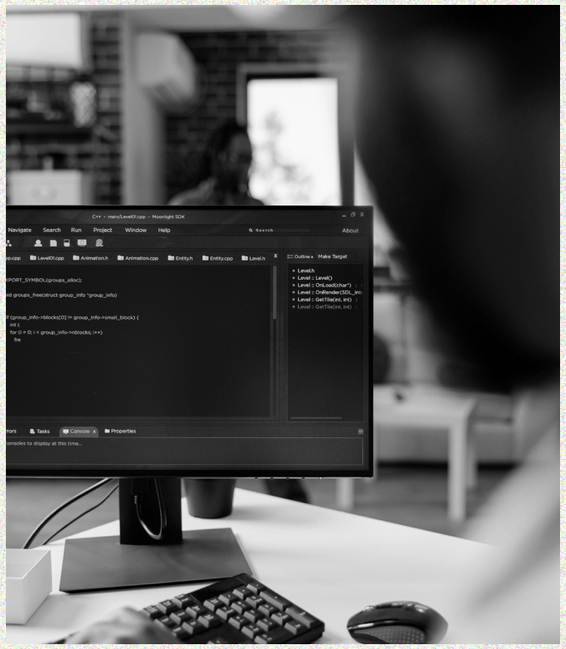


1.1. PANORAMA DE **AMENAZAS**

Actualmente en el contexto en que nos movemos las principales amenazas en ciberseguridad se enmarcan en un entorno digital en constante y rápida evolución, donde las tecnologías, las organizaciones, personas y la sociedad evolucionan rápidamente y dependen cada vez más de sistemas conectados entre sí.

En este contexto las amenazas de ciberseguridad impulsadas por la rápida evolución tecnológica, el aumento de la digitalización y la creciente sofisticación tanto de los ataques como de los atacantes ha hecho que las organizaciones tengan que adoptar un enfoque más proactivo con respecto a la ciberseguridad incluyendo la implementación de nuevas tecnologías, la capacitación y formación continua de sus empleados, al igual que, también han tenido que adaptar la organización a los desafíos regulatorios que se están dando y que se avecinan en el corto y medio plazo.

A continuación, realizamos una descripción más detallada de las amenazas a las que nos enfrentamos, como son:



- **Amenazas Geopolíticas:** Las tensiones geopolíticas han llevado a un aumento en los ataques patrocinados por estados, donde los actores estatales buscan desestabilizar a otros países o robar información estratégica. Esto ha llevado a un aumento en la sofisticación y la frecuencia de los ataques, afectando tanto a organizaciones gubernamentales como a empresas privadas.

- **La Digitalización:** La transformación digital ha llevado a muchas organizaciones a adoptar tecnologías en la nube, IoT, Inteligencia Artificial, etc. Esto ha ampliado la superficie de ataque, creando más oportunidades para los atacantes.

- **Evolución de las Técnicas de Ataque:** Actualmente se están utilizando por parte de los atacantes nuevas técnicas más sofisticadas, como el empleo de inteligencia artificial (IA) y machine learning (ML) para automatizar ataques y evadir su detección, así como el empleo de técnicas de phishing que se han vuelto más personalizadas y difíciles de identificar. Esto ha llevado a un aumento en la efectividad de los ataques, lo que hace que las organizaciones sean más susceptibles a tener incidentes de seguridad.

- **Regulaciones y Cumplimiento:** Las organizaciones se enfrentan a un entorno regulatorio cada vez más estricto en torno a la protección de datos, como GDPR en Europa y otras leyes de privacidad en todo el mundo. El incumplimiento puede resultar en sanciones y daños a la reputación de las empresas, lo que aumenta la presión sobre las empresas para mejorar su nivel de seguridad.

1.2. RETOS DE SEGURIDAD **PARA LAS EMPRESAS**

Ante un panorama como el descrito anteriormente, no cabe duda que, las organizaciones se enfrentan a desafíos sin precedentes en el ámbito de la ciberseguridad, esto es debido a la rápida evolución de las tecnologías, el aumento del número de vulnerabilidades descubiertas, así como la adopción de nuevas tecnologías en el ámbito de las organizaciones.

Todo este panorama, hace que la gestión de las operaciones de seguridad y tecnología, se vuelvan más complejas, los responsables de seguridad, así como los equipos operativos deben adaptarse a este escenario cada vez más dinámico y cambiante.

Para ilustrarlo mejor, a continuación, se destacan algunos de los nuevos retos a los que se enfrentan las organizaciones:

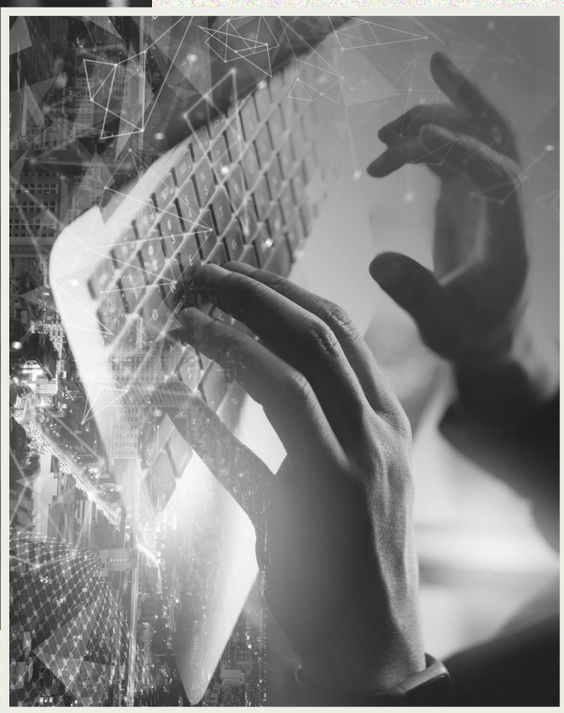
- **Recursos Limitados:** casi todas las empresas y especialmente las que son pequeñas y medianas, no disponen de los recursos financieros y humanos necesarios para implementar medidas de ciberseguridad adecuadas. La priorización en las inversiones ciberseguridad y la búsqueda de soluciones rentables que se ajusten a su presupuesto, es uno de los retos a los que se enfrentan.
- **Complejidad Tecnológica:** el empleo de una combinación de sistemas heredados junto con la incorporación de nuevas tecnologías pueden complicar la gestión de la seguridad. Desarrollar una estrategia integral de ciberseguridad que aborde la diversidad de la infraestructura tecnológica significa un reto que las organizaciones deben abordar.
- **La Gestión de Proveedores y Terceros:** las organizaciones tienen una dependencia cada vez mayor de proveedores y socios que pueden ser vulnerables a ciertos tipos de ataque como el eslabón más débil en la cadena de suministro. La evaluación y gestión de los riesgos de ciberseguridad asociados con terceros, asegurando que cumplan con los estándares de seguridad, supone uno de los mayores retos para las organizaciones.
- **Resiliencia ante Incidentes:** la capacidad de una empresa para recuperarse de un incidente de ciberseguridad es crucial, pero muchas organizaciones no tienen planes de respuesta adecuados, que permitan disponer de planes en caso de un incidente que afecte a la operativa de la organización. Desarrollar y probar regularmente planes de respuesta a incidentes y estrategias de recuperación ante desastres, es fundamental.
- **Escasez de Talento:** existe una alta demanda de profesionales de ciberseguridad Atraer y retener talento en ciberseguridad, así como invertir en la formación y desarrollo de habilidades del personal existente es fundamental para hacer frente a los nuevos retos.

En este escenario, la ciberseguridad ya no puede abordarse únicamente como un asunto operativo, sino como un elemento central en la agenda estratégica de la organización. La complejidad de las amenazas, sumada a la creciente dependencia de infraestructuras digitales y servicios críticos, obliga a las compañías a adoptar un enfoque proactivo, con capacidades de monitorización, detección y respuesta en tiempo real.

Disponer de un centro de operaciones de seguridad (SOC) deja de ser una opción para convertirse en un pilar estratégico, que no solo protege los activos más valiosos, sino que también respalda la continuidad del negocio y la confianza de clientes, socios y reguladores.

Sobre cómo llevar a la práctica este modelo y cuáles son los factores clave de éxito en su implementación, resulta fundamental conocer la visión de los expertos en ciberseguridad, quienes aportan un conocimiento profundo del terreno y una experiencia decisiva en la construcción de estas capacidades.

¿QUÉ OPINAN LOS PROFESIONALES DE LA SEGURIDAD?



En una organización, proteger los activos críticos no es un ejercicio uniforme: cada perfil implicado en la ciberseguridad interpreta riesgos, prioridades y responsabilidades desde una óptica distinta. Comprender estas perspectivas es fundamental para alinear esfuerzos, reducir silos y avanzar hacia un modelo de defensa que responda de manera integrada a las exigencias del negocio. Tarea imprescindible para lograr que un centro de operaciones de seguridad (SOC) sea efectivo y cumpla con su misión, visión y objetivos.

En la tabla que sigue se presentan las visiones de distintos actores esenciales en la gestión de la seguridad. Esta comparación permite identificar tanto sus diferencias como sus áreas de convergencia, ofreciendo una base sólida para construir un punto de entendimiento a la hora de proteger la organización.

Además, este entendimiento compartido sirve como antesala natural a la introducción del concepto de Security Operations Center (SOC): un entorno en el que no solo se gestionan alertas y amenazas, sino donde confluyen las distintas perspectivas para traducirse en procesos, tecnología y métricas alineadas con los objetivos del negocio. Este es el punto de partida para evolucionar desde una visión fragmentada hacia un modelo orquestado y verdaderamente estratégico de ciberseguridad.

DIMENSIÓN	CISO	LÍDER DE SOC	INGENIERO DE SEGURIDAD
ENFOQUE	ESTRATEGIA Y GOBERNANZA	EFICIENCIA OPERATIVA	IMPLEMENTACIÓN TÉCNICA
PRIORIDADES	REDUCCIÓN DE RIESGOS, ALINEACIÓN CON OBJETIVOS DE NEGOCIO	MTTD/MTTR, PROCEDIMIENTOS REPETIBLES	INVESTIGACIÓN DE INCIDENTES, CONTROLES DE DEFENSA
HERRAMIENTAS CLAVE	VISIBILIDAD EN TIEMPO REAL, MÉTRICAS DE MADUREZ	AUTOMATIZACIÓN, RESPUESTAS, CONTENCIÓN	ANÁLISIS DE LOGS, SIMULACIONES DE ATAQUE
RETOS PRINCIPALES	CULTURA DE SEGURIDAD DECISIONES BASADAS EN DATOS	FATIGA DE ALERTAS, FORMACIÓN CONTINUA	ADAPTACIÓN A NUEVAS AMENAZAS, COLABORACIÓN CON OTROS EQUIPOS
INDICADORES DE ÉXITO	REDUCCIÓN DE INCIDENTES, CUMPLIMIENTO NORMATIVO	TIEMPO DE RESPUESTA, EFICIENCIA DEL EQUIPO	PRECISIÓN EN LA DETECCIÓN, REDUCCIÓN DE VULNERABILIDADES
INTERACCIÓN CON OTROS ROLES	ALTA DIRECCIÓN, EQUIPOS DE NEGOCIO, AUDITORIA	ANALISTAS DE SOC, EQUIPOS DE RESPUESTA A INCIDENTES, DPO	IT, DESARROLLO, COMPLIANCE

2.1. VISIÓN DE UN **CISO**

En el ecosistema actual de Ciberseguridad, el rol del CISO ha evolucionado de forma notable. Ya no se trata únicamente de un perfil técnico que vela por la protección de los sistemas informáticos, sino de una figura estratégica que actúa como garantía de la organización. En España, donde la presión regulatoria (NIS2, ENS, DORA) y la exposición a amenazas globales van en aumento, el CISO se ha convertido en un actor clave en la toma de decisiones corporativas.

¿Qué hace este rol?

El CISO es quien define la estrategia de seguridad de la organización. Su responsabilidad principal es garantizar que los riesgos estén identificados, evaluados y gestionados de forma coherente con los objetivos del negocio. Esto implica diseñar políticas, liderar planes de concienciación, supervisar auditorías, y coordinar tanto equipos internos como proveedores externos. Aunque no se involucra directamente en la operación técnica diaria, sí toma decisiones que afectan a todo el ecosistema de la empresa.

En muchas organizaciones españolas, el CISO reporta directamente al comité de dirección o al CIO, y su influencia se extiende más allá del departamento de IT. Su rol es transversal, como: asegurar que la seguridad esté presente desde el diseño de productos hasta la relación con terceros, pasando por la protección de datos personales, la continuidad operativa y de negocio.

¿Qué quiere conseguir?

El objetivo del CISO es reducir el riesgo sin frenar la innovación. Busca que la organización esté preparada para responder a incidentes, cumplir con las normativas vigentes y adaptarse a nuevas exigencias regulatorias. También quiere que la seguridad sea entendida y valorada por toda la empresa, no solo por el equipo técnico.

En términos prácticos, esto se traduce en lograr una postura de seguridad madura, con procesos definidos, métricas claras y una capacidad de respuesta eficaz. El CISO aspira a que la seguridad sea parte del ADN de la organización.

¿Cómo ve la seguridad?

Para el CISO, la seguridad no es un gasto, sino una inversión estratégica. Es una palanca de confianza, reputación y cumplimiento. Su visión es holística: la seguridad debe estar integrada en todos los procesos, no añadirse como un parche. La concibe como un habilitador del negocio, no como un freno. Esto implica trabajar con una mentalidad de seguridad desde el arranque (recientemente se escucha “security by design”) y fomentar una cultura organizativa donde todos los empleados entiendan su papel en la protección de la información.

Además, el CISO entiende que la seguridad no es estática. Las amenazas evolucionan, los modelos de negocio cambian, y la tecnología avanza. Por eso, su enfoque es dinámico, basado en la mejora continua y en la anticipación.

¿Con quién se relaciona?

El CISO actúa como un conector entre mundos. Se relaciona con la alta dirección para alinear la estrategia de seguridad con los objetivos corporativos. Colabora con IT para asegurar que la infraestructura esté protegida desde el diseño. Trabaja con legal para garantizar el cumplimiento normativo. Y, por supuesto, también se coordina cuando es necesario con entiedades externas como INCIBE, CCN-CERT, etc. En este sentido, su capacidad de comunicación es tan importante como su conocimiento técnico. Debe saber traducir riesgos complejos en términos comprensibles para los decisores, y al mismo tiempo, inspirar confianza en los equipos operativos.

¿Qué herramientas o habilidades necesita?

Más allá de las herramientas técnicas, el CISO necesita visibilidad. Reportes de riesgos, informes de madurez, mapas de amenazas, y métricas de cumplimiento son esenciales para tomar decisiones informadas. También requiere habilidades de liderazgo, gestión de crisis, negociación y comunicación.

En el contexto español, donde muchas organizaciones están en proceso de transformación digital, el CISO debe ser capaz de liderar ese cambio desde la seguridad, integrando nuevas tecnologías (cloud, IA, IoT) sin comprometer la protección.

¿Cómo sabe si lo está haciendo bien?

El éxito del CISO no se mide solo en la ausencia de incidentes, sino en la capacidad de la organización para anticiparse, resistir y recuperarse. Indicadores como el tiempo medio de detección y respuesta (MTTD/MTTR), el número de incidentes críticos evitados, el grado de cumplimiento normativo o la madurez del programa de concienciación son claves.

Pero también hay señales más cualitativas: que la dirección consulte al CISO antes de lanzar un nuevo producto, que los empleados reporten incidentes de forma proactiva, o que los auditores reconozcan la solidez del modelo de seguridad.

¿Qué le complica la vida?

Entre los principales retos del CISO se encuentran la falta de cultura de seguridad en la organización, la presión por justificar presupuestos, y la dificultad de medir el retorno de la inversión en seguridad. También le preocupa la fragmentación de herramientas, la escasez de talento especializado y la dependencia de proveedores que no siempre entienden el contexto del negocio.

Además, la creciente complejidad normativa (ENS, NIS2, DORA, GDPR) exige coordinación constante con áreas legales y de cumplimiento, lo que añade una capa adicional de responsabilidad.

¿Qué cree que viene en el futuro?

El CISO ve un futuro donde la seguridad será aún más estratégica. La automatización, la inteligencia artificial y la analítica avanzada permitirán una gestión más proactiva del riesgo. Al mismo tiempo, la presión regulatoria y la sofisticación de los ataques exigirán una mayor coordinación entre áreas.

El rol del CISO será cada vez más híbrido: parte tecnólogo, parte gestor, parte comunicador. Su éxito dependerá de su capacidad para liderar en la incertidumbre, construir alianzas internas y externas, y mantener la confianza en un entorno cada vez más complejo.

A la vista de lo expuesto anteriormente, y desde la perspectiva de un CISO, un Centro de Operaciones de Seguridad no es meramente una capacidad técnica, sino un pilar fundamental para la resiliencia organizacional en un entorno de amenazas en constante evolución.

Para el CISO, el SOC es una herramienta que le proporciona una consciencia situacional completa, y lo convierten en un socio estratégico en su labor diaria para la protección de la organización.

2.2. VISIÓN DE UN **SOC LEADER**

¿Qué hace este rol?

El SOC Leader (a veces llamado SOC Manager o SOC Director) es la figura responsable de dirigir al equipo de analistas de seguridad encargados de monitorizar, detectar y responder a las amenazas diarias. A nivel de gestión, coordina turnos, asigna recursos y prioriza alertas según el riesgo. Además, tiene como tarea la mejora continua de procedimientos y la integración de nuevas tecnologías. Pero no sólo esto, el SOC Leader juega un papel fundamental como enlace entre el SOC y la organización.

Aunque pueda parecer que es una figura meramente técnica, el rol del SOC Leader es un perfil muy completo que debe tener capacidad técnica, conocimiento del panorama de amenazas pero, sobre todo, debe disponer de una dualidad de lenguaje que le permita hablar tanto a nivel técnico como de negocio.

¿Cuál es su papel dentro del equipo de seguridad?

Tiene un papel intermediario entre en el equipo de analistas/especialistas-ingenieros y la dirección de seguridad (CISO). Su papel incluye:

- Que el SOC cumpla con los SLA (Acuerdos de Nivel de Servicio) y los KPI (Indicadores Clave de Rendimiento).
- Traducir las necesidades estratégicas del CISO en acciones operativas.
- Fomentar la coordinación entre los distintos profesionales del SOC para que trabajen de forma unificada bajo los mismos criterios y procedimientos

¿Qué tipo de decisiones toma y por qué son importantes?

Estas decisiones son importantes por que afectan directamente a la capacidad de respuesta ante incidentes de seguridad y la eficiencia del equipo.

- **Asignación de recursos:** gestiona cuantos analistas cubren cada turno según la carga de trabajo dentro y fuera de horas.
- **Priorización de incidentes:** determina que alertas requieren atención inmediata basándose en la peligrosidad e impacto.
- **Punto de referencia en inversión:** para nuevas herramientas puede decidir cual se adapta más a las necesidades del SOCcomo por ejemplo la automatización (SOAR), entre otras muchas.

¿Cómo ve la seguridad?

El SOC Leader ve la seguridad como parte de una estrategia integral que afecta a la empresa, no solo como un conjunto de herramientas. La seguridad debe:

- Adaptarse a la evolución de amenazas
- Integrarse con los procesos de negocio
- Ser valorada en términos de reducción de riesgos, no solo en detección de incidentes

¿Qué significa “hacer bien su trabajo” desde su punto de vista?

- Eficiencia operativa: reducir falsos positivos y tiempos de respuesta
- Madurez del SOC: transformando las operaciones improvisadas, no documentadas, hacia procesos consistentes, repetibles y medibles.Alta disponibilidad: garantizar cobertura 24/7 sin sobrecargar al equipo.

¿Qué quiere conseguir?

Para un líder de un Centro de Operaciones de Seguridad (SOC), sus objetivos abarcan un espectro que va desde la estrategia organizacional hasta la gestión operativa diaria.

Uno de los objetivos primordiales de un SOC Leader, es la consecución de la alineación estratégica con negocio, lo que implica definir y comunicar claramente la misión, visión y responsabilidades de un SOC, asegurando que esta encaja perfectamente con los objetivos empresariales de la organización a proteger.

En el ámbito de la **gestión de personas**, el líder del SOC tiene como objetivo clave atraer, desarrollar y retener personal de alta calidad. Esto incluye establecer procesos de reclutamiento y estrategias de retención, definir roles y responsabilidades claras, e implementar programas de capacitación y certificación que aseguren las habilidades y conocimientos requeridos.

Desde una perspectiva de **procesos y operaciones,** el líder busca formalizar las operaciones de ciberseguridad, evolucionando de un enfoque ad-hoc a uno sistemático y documentado. Esto se logra mediante la creación y mantenimiento de procesos operativos estandarizados, que aseguran una entrega de servicios de alta calidad y ajustados a las necesidades de su cliente.

Sin olvidar la gestión operativa del SOC que comprende aspectos de mejora como:

- Asegurar una monitorización eficaz, realizando aquellas acciones que se consideren para disponer de una visión lo más completa posible de los activos de la organización.
- Garantizar la priorización adecuada de las alertas
- Mejorar los tiempos de detección y respuesta de incidentes de seguridad
- Desarrollar y mantener los procesos operativos del SOC
- Automatizar aquellas tareas repetitivas que se dan cita en las fases de triaje e investigación
- Definir, medir e informar adecuadamente los resultados de los KPIs del SOC
- Etc.

¿Con quién se relaciona?

Internamente:

- **CISO:** Alineando las operaciones del SOC con la estrategia de ciberseguridad y reporte de métricas.
- **Equipo de analistas y especialistas:** Asegurando la comunicación interna y ejecución de procedimientos que tienen que aplicar para la gestión de alertas.
- **Equipos de IT:** Coordinando respuesta a incidentes que afecten a la infraestructura.
- **Equipo de GRC:** Asegurando que el SOC cumple con las regulaciones en términos de seguridad y políticas internas
- **Legal y RRHH:** Participando en investigaciones de brechas que involucren exfiltración de datos sensibles, y en procesos de selección.

Externamente:

Proveedores de seguridad: En el tratamiento de casos con fabricante, evaluación de herramientas y colaboración con otros departamentos para negociación.

CCN CERT, INCIBE y Fuerzas de seguridad: Colaborando en ataques avanzados (ej. APTs) o fraudes nacionales.

¿Qué herramientas o habilidades necesita?

El rol de SOC Leader requiere un balance entre perfil técnico y gerencial. En este balance se tiene encuentran herramientas técnicas y habilidades sociales y estratégicas:

- **Herramientas técnicas:** Conocimientos en redes y sistemas, ticketing, compliance y herramientas de seguridad: SIEM, EDR, WAF y SOAR mayormente.
- **Habilidades sociales:** Liderazgo situacional (motivar a los equipos en momentos de crisis) y comunicación asertiva (explicar riesgos técnicos a alta dirección).
- **Habilidades estratégicas:** Gestión de métricas (traducción de datos técnicos a lenguaje de negocio) y presupuestación (justificar inversiones basándose en reducir costes de remediación).

¿Qué le complica la vida?

El SOC Leader se enfrenta a obstáculos comunes con los que tiene que convivir como: Sin olvidar la gestión operativa del SOC que comprende aspectos de mejora como:

- **Escasez de talento:** La alta demanda de analistas para SOC (especialmente con skills en cloud o IA) dificulta la búsqueda de perfiles cualificados técnicamente.
- **Fatiga por volumetría:** Casos de uso / Reglas mal afinadas en el SIEM generan falsos positivos, desgastando al equipo.
- **Expectativa vs Realidad:** La alta dirección espera “protección total”, pero el SOC trabaja en un modelo de riesgo aceptable.
- **Integración:** Herramientas desconectadas, por ejemplo, un EDR que no comparte datos con el SIEM.

¿Cómo sabe si lo está haciendo bien?

¿Qué indicadores o métricas usa para medir su impacto?

— **Operativas:** Tiempo de reacción y notificación y tasa de falsos positivos.

— **Estratégicas:** ROI del SOC (Coste vs pérdidas evitadas) y Satisfacción del cliente interno/externo.

¿Cómo demuestra su valor al resto de la organización?

— **Reportes ejecutivos:** dashboards con tendencias de ataques en tu propia organización Simulacros y ejercicios: Pruebas con ataques controlados para saber si se responde en tiempo y forma y se documenta adecuadamente el proceso.

— **Participación en auditorías:** Mostrar como el SOC contribuye al cumplimiento de normativas nacionales e internacionales.

¿Qué cree que viene en el futuro?

El rol de SOC Leader se trasladará hacia un punto de vista de estrategia transversal. Tendrá que contar con habilidades técnicas, de negocio y comunicativas. Como puntos importantes que moldearán el rol serían:

Automatización extrema (Hyperautomatización)

— **Generative AI para análisis de logs:** Copilot, Gemini o ChatGPT para resumen de incidentes en lenguaje natural y generación de reportes ejecutivos.

— **Autoremediación:** Capacidad de toma de decisiones autónomas (ej., aislar equipos infectados sin intervención humana, bloqueo de IOCs en base a fuentes de inteligencia confiables, etc).

Consolidación de tecnologías:

— **XDR (Extended Detection and Response):** Unificación de visibilidad en endpoints, redes y cloud.

— **CNAPP (Cloud-Native Application Protection Platforms):** Dominar la seguridad en entornos multi-cloud (AWS/Azure/GCP).

SOCaaS y Equipos Híbridos

— **Externalización parcial:** Empresas medianas adoptarán SOC como servicio, pero el SOC Leader retendrá el control de la estrategia.

— **Equipos globales 24/7:** Analistas en remoto con turnos escalonados (ej.: seguimiento de amenazas desde LATAM, Europa y Asia).

Regulaciones y Compliance ÁgilA

— **Adaptación a nuevas leyes:** Ej.: IA Act (UE), normas de soberanía de datos.

— **SOC como auditor interno:** Verificación continua de cumplimiento (ej.: Zero Trust en frameworks como NIST 800-207).

En general, la coordinación del SOC observa una evolución clara hacia operaciones asistidas por inteligencia artificial generativa, con analistas virtuales (agentes de IA) capaces de resumir incidentes y proponer acciones. Se prevé una mayor consolidación tecnológica y una adopción más amplia de servicios híbridos o externalizados. También gana peso la idea de entornos diseñados para contener y estudiar ataques sin comprometer los activos reales, como complemento a la detección tradicional.

2.3. VISIÓN DE UN **INGENIERO DE SEGURIDAD**

En el engranaje de un Centro de Operaciones de Seguridad (SOC), el ingeniero de seguridad representa la capa más cercana a la acción. Es quien traduce la estrategia en medidas concretas, quien responde ante las alertas, quien analiza los logs, y quien, en definitiva, se enfrenta cara a cara con las amenazas. Su rol es técnico, sí, pero también es profundamente analítico, resolutivo y colaborativo.

¿Qué hace este rol?

El ingeniero de seguridad es el responsable de implementar, mantener y mejorar los controles técnicos que protegen los activos de la organización. Su trabajo abarca desde la configuración de firewalls, sistemas de detección y protección, hasta el análisis forense de incidentes, la gestión de vulnerabilidades o la automatización de respuestas. Es quien está "en la trinchera", monitorizando eventos, investigando comportamientos anómalos y aplicando medidas correctivas.

Además, participa en la definición de reglas de correlación, en la creación de modelos/configuración de detecciones avanzadas, e incluso en la integración de nuevas fuentes de datos en el SIEM. En muchos casos, también colabora en pruebas de penetración, simulaciones de ataque (red teaming) o ejercicios de respuesta a incidentes.

¿Qué quiere conseguir?

Su objetivo es claro: proteger los sistemas y datos de la organización de forma eficaz y sostenible. Quiere reducir el número de falsos positivos, mejorar la detección de amenazas reales, y automatizar tareas repetitivas para centrarse en lo que realmente importa. También busca que las herramientas estén bien integradas, que los procedimientos sean claros, y que el equipo trabaje de forma coordinada.

Además, aspira a que su trabajo tenga impacto: que las recomendaciones que hace se apliquen, que las vulnerabilidades que detecta se corrijan, y que las lecciones aprendidas de cada incidente se traduzcan en mejoras reales.

¿Cómo ve la seguridad?

Para el ingeniero de seguridad, la seguridad es un sistema vivo. No es una política en un documento, sino un conjunto de mecanismos que deben funcionar en tiempo real, bajo presión y con precisión. La ve como un reto técnico, pero también como una responsabilidad: sabe que un fallo en su configuración puede tener consecuencias graves.

Su visión es pragmática: lo importante es que las defensas funcionen, que las alertas sean útiles, que las respuestas sean rápidas. No busca la perfección teórica, sino la eficacia operativa. Y, sobre todo, entiende que la seguridad es un proceso continuo, no un estado final.

¿Con quién se relaciona?

Aunque su trabajo es técnico, el ingeniero de seguridad no trabaja solo. Colabora estrechamente con analistas, administradores de sistemas, equipos de redes, desarrolladores y, en ocasiones, con personal de IT o incluso de negocio. También interactúa con el CISO o el líder de SOC para reportar hallazgos, proponer mejoras o escalar incidentes.

En entornos con servicios externalizados, puede coordinarse con proveedores de seguridad gestionada (MSSP), revisando tickets, validando alertas o solicitando acciones específicas. Su capacidad de comunicación es clave para que las acciones técnicas se entiendan y se ejecuten correctamente.

¿Qué herramientas o habilidades necesita?

El ingeniero de seguridad necesita un dominio profundo de herramientas como SIEM, EDR, firewalls, escáneres de vulnerabilidades, sistemas de sandboxing, y plataformas de threat intelligence. También debe saber programar (Python, Bash, PowerShell), entender protocolos de red, y tener conocimientos sólidos de sistemas operativos, tanto Windows como Linux.

Pero más allá de lo técnico, necesita habilidades de análisis, pensamiento crítico, capacidad de priorización y, cada vez más, conocimientos de automatización y orquestación (SOAR). En el contexto español, donde muchas organizaciones están adoptando modelos híbridos y multicloud, también es clave que entienda arquitecturas distribuidas y entornos cloud (Azure, AWS, GCP).

¿Cómo sabe si lo está haciendo bien?

El ingeniero de seguridad mide su éxito en términos de eficacia operativa: reducción de falsos positivos, tiempo medio de investigación, número de incidentes resueltos, calidad de los informes técnicos. También valora que sus recomendaciones se apliquen, que sus scripts se reutilicen, y que su trabajo sea reconocido por el equipo.

En algunos casos, participa en KPIs más amplios definidos por el SOC o el CISO, pero su foco está en la calidad técnica y en la mejora continua. Si el entorno es más seguro, más estable y más predecible gracias a su trabajo, sabe que va por buen camino.

¿Qué le complica la vida?

Entre los principales retos del ingeniero de seguridad están la sobrecarga de alertas, la falta de contexto en los eventos, y la presión por responder rápido sin margen de error. También le afecta la fragmentación de herramientas, la escasa documentación de algunos entornos, y la falta de tiempo para tareas de mejora continua.

Otro factor crítico es la falta de visibilidad: si no tiene acceso a ciertos logs, si las integraciones no funcionan bien, o si los sistemas no están bien configurados, su capacidad de detección se ve limitada. Además, en muchas organizaciones, las decisiones de seguridad se toman sin consultar al equipo técnico, lo que genera frustración y desconexión.

¿Qué cree que viene en el futuro?

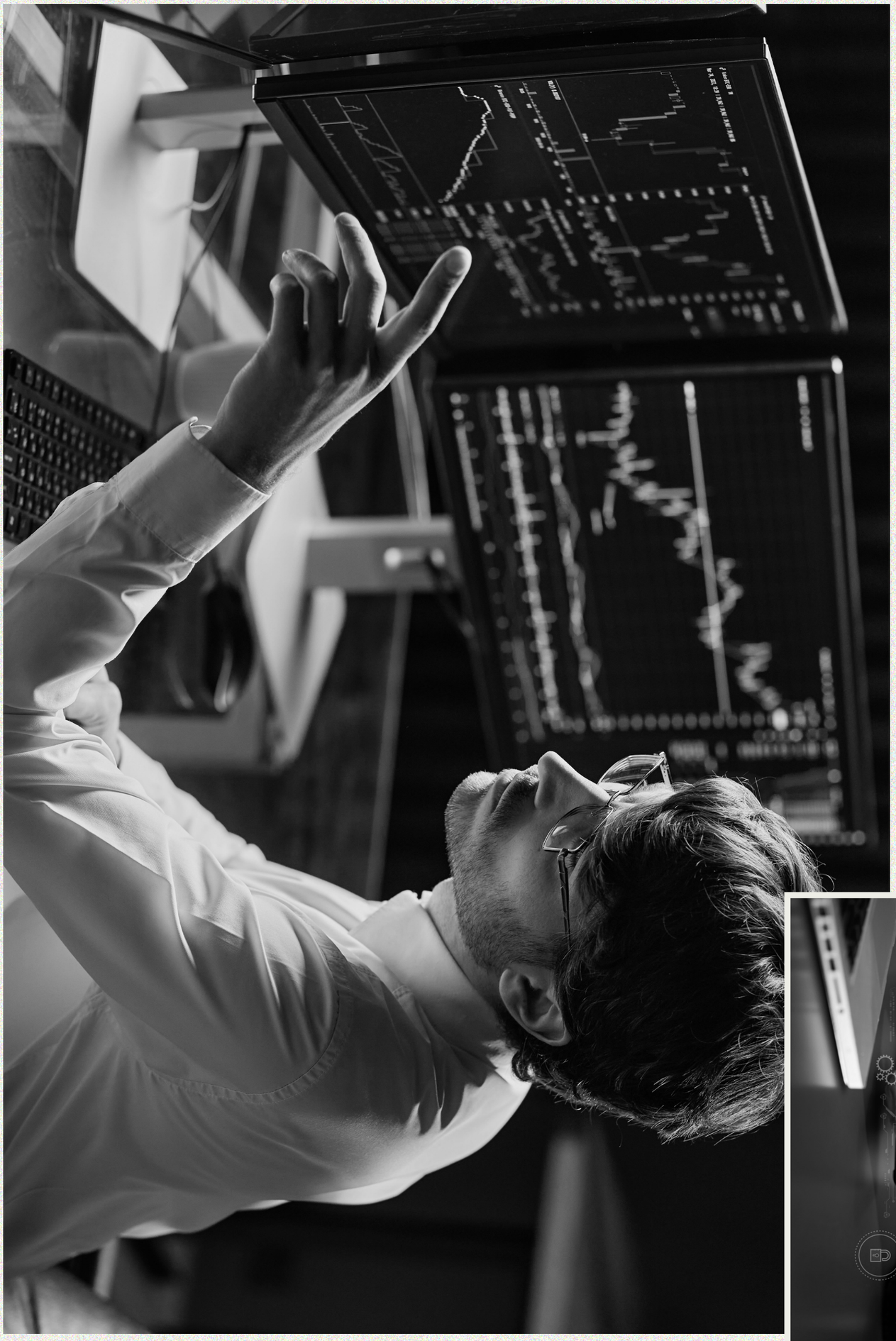
El ingeniero de seguridad ve un futuro donde la automatización será clave. Las tareas repetitivas serán asumidas por sistemas inteligentes, y su rol se centrará en la investigación avanzada, la ingeniería defensiva y la adaptación a nuevas amenazas. También anticipa una mayor integración entre seguridad y desarrollo (DevSecOps), y una necesidad creciente de entender entornos cloud y arquitecturas distribuidas.

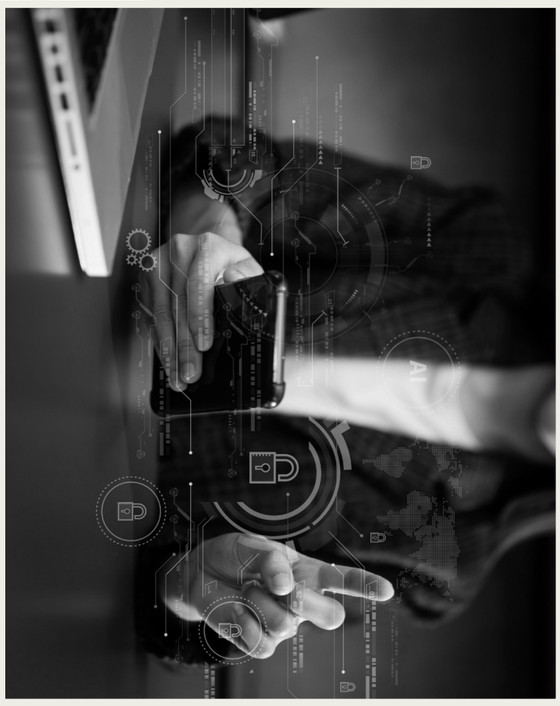
Además, cree que su perfil será cada vez más valorado, pero también más exigente: deberá aprender constantemente, adaptarse a nuevas herramientas, y colaborar con perfiles muy diversos. En definitiva, será un profesional técnico, pero también estratégico, capaz de construir defensas sólidas en un mundo cada vez más complejo.

Por otra parte, se vislumbra un escenario dominado por la automatización, el análisis proactivo y la integración nativa de sistemas. Se esperan avances en detección contextual, reducción de falsos positivos y capacidades de respuesta autónoma. Cada vez se valora más el uso de redes espejo o entornos virtuales engañosos donde el atacante puede ser observado sin riesgo para los sistemas reales, reforzando así la capacidad de aprendizaje frente a amenazas reales.

3.

ACLARANDO TÉRMINOS





En el paradigma de la ciberseguridad actual, ya sea a nivel interno dentro de las organizaciones, como de aquellas empresas de este sector cuya base de negocio es proporcionar servicios a terceros, es común encontrarse con términos como SOC, CERT y CSIRT.

Aunque suelen utilizarse indistintamente, cada uno de ellos dispone de una representatividad distinta relacionada con las funciones, estructura y enfoque dentro de la gestión de incidentes de seguridad. Es por esto por lo que conocer sus puntos comunes y diferencias es esencial para conseguir:

— Establecer un lenguaje común, identificando cuáles son sus objetivos principales y como se relacionan entre sí en el ecosistema de la ciberseguridad.

— Organizar eficazmente una estrategia de defensa eficiente dentro de la organización.

— Definir roles y responsabilidades, así como la rendición de cuentas alrededor de los procesos de detección y respuesta a incidentes.

3.1. DEFINIENDO CADA **TÉRMINO**

SOC vs CERT vs CSIRT

El SOC, o centro de operaciones de seguridad, tiene como función principal ofrecer un servicio de detección temprana de incidentes mediante la observación de eventos técnicos en redes y sistemas. En las grandes empresas, los SOC a veces se centran sólo en los servicios de supervisión y detección, y luego traspasan la gestión de incidentes a un CSIRT independiente. En organizaciones más pequeñas, los CSIRT y los SOC suelen considerarse sinónimos.

Normalmente, los equipos SOC suelen evolucionar a partir de equipos de seguridad de tecnologías de la información (TI) que automatizan su trabajo utilizando información de seguridad y gestión de eventos (SIEM) y otras tecnologías de automatización y orquestación de la seguridad para la supervisión de la seguridad (SOAR).

Para garantizar un alto grado de servicio, el funcionamiento del SOC suele estar relacionado con parámetros de rendimiento como la velocidad de detección, volumen de alertas o eventos analizados (carga de trabajo), número de escalados, cobertura y tasa de falsos positivos entre otros.

En los últimos años, muchas organizaciones han optado por externalizar parte o la totalidad de sus operaciones de seguridad mediante SOC's comerciales o proveedores de servicios gestionados de seguridad (MSSP). Esta tendencia responde a la creciente complejidad del panorama de amenazas y a la escasez de profesionales altamente cualificados en ciberseguridad. Los MSSP permiten a las empresas contar con capacidades avanzadas de monitorización, detección y respuesta sin necesidad de mantener un equipo interno especializado. Esta solución resulta particularmente atractiva para pequeñas y medianas empresas que no pueden asumir los costes y recursos que implica operar un SOC interno 24/7, pero que aun así necesitan proteger sus activos críticos frente a incidentes de seguridad, así como operar las soluciones de seguridad implantadas.

CSIRT significa Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática), sin embargo, un CSIRT no es solo un equipo de respuesta a incidentes; es el núcleo estratégico que fortalece la resiliencia, fomenta la prevención y coordina la defensa integral de una organización contra las amenazas cibernéticas.

Para explicar lo que es un CSIRT, o cuál es su esencia, vamos a tomar como referencia la forma en la que los diversos organismos de referencia hacen su definición. Según esto:

FIRST o Foro de Equipos de Respuesta a Incidentes y Seguridad,

es una organización de ámbito internacional de coordinación y colaboración de centros de respuesta (ver punto 8 de esta guía). Para el FIRST la definición de un centro de respuesta antes incidentes, o CSIRT, se relaciona de forma directa con los servicios que proporciona.

Conscientes de la necesidad de poder disponer de una estandarización de equipos y funciones que de alguna forma sirva de lenguaje común para el mercado, FIRST desarrolla y publican un trabajo relacionado con un framework de definición de servicios.

El framework tiene como objetivo principal, proporcionar una visión de alto nivel de las áreas de servicio, funciones y subfunciones que podrían estar englobadas en los equipos encargados de la respuesta a incidentes.

De acuerdo con este, los servicios se organizan en cinco grandes áreas:

— Gestión de eventos de seguridad la información.

— Gestión de incidentes de seguridad de la información

— Gestión de vulnerabilidades

— Consciencia coyuntural

— Transferencia de conocimientos.

Ref: Forum of Incident Response and Security Teams. (2019). CSIRT Services Framework Version 2.1. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

ENISA (European information security agency):

Según ENISA, un CSIRT es un equipo al que se asigna la gestión de incidentes de seguridad informática y/o ciberseguridad. A menudo esto incluye responsabilidades adicionales, desde la detección hasta el análisis, e incluso la reparación práctica, así como diferentes actividades de conocimiento de la situación, transferencia de conocimientos y gestión de vulnerabilidades. A lo largo de los años, el papel de un CSIRT ha evolucionado desde la prestación de servicios de supervisión y gestión de incidentes hasta la coordinación y comunicación con diferentes partes interesadas, países y sectores específicos.

Así desde ENISA se establece una relación entre la definición de lo que es un CSIRT con las funciones que lo representan, concluyendo que el término CSIRT se ha convertido en una denominación genérica para un equipo que proporciona diversos servicios (gestión de incidentes de información y ciberseguridad (servicio principal), supervisión de la seguridad, gestión de vulnerabilidades, conocimiento de la situación y gestión del conocimiento sobre ciberseguridad, estableciendo una alineación de los mismos y una referencia clara nuevamente al framework diseñado por FIRST.

TF-CSIRT (Task Force - Computer Security Incident Response Teams):

Al igual que FIRST, TF-CSIRT representa una comunidad de equipos de respuesta a incidentes (ver punto 8 de esta guía), en este caso a nivel europeo. Como en el caso de FIRST la definición del CSIRT se realiza en función de los servicios que este presta a la comunidad, no en vano TF-CSIRT ha sido colaborador con FIRST en la definición del framework de servicio.

Foro CSIRT.es

El Foro CSIRT.es (ver punto 8 de esta guía) es una plataforma independiente de confianza y sin ánimo de lucro compuesto por aquellos equipos de respuesta a incidentes de seguridad informáticos cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra dentro del territorio español.

Ref: European Union Agency for Cybersecurity (ENISA). (2020). How to set up CSIRT and SOC. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

Para pertenecer al Foro y por tanto ser considerado un CSIRT, los equipos deben proporcionar algún tipo de servicio relacionado con la atención de incidentes de seguridad, tales como: análisis de incidentes, respuesta a Incidentes de seguridad y/o soporte en la respuesta a incidentes.

Por otro lado, los CSIRT también se conocen como:

CIRT (equipos de respuesta a incidentes informáticos).
CERT (equipos de respuesta a emergencias informáticas).
SIRT (equipos de respuesta a incidentes de seguridad).

Adicionalmente, los equipos nacionales también pueden denominarse centros nacionales de ciberseguridad (CNSC), que por ley suelen tener asignada la función de CSIRT, además de prestar servicios adicionales para la nación (por ejemplo, gestionar los esquemas de clasificación de la información de un país).

Centrándonos más en el término CERT, este hace referencia Computer Emergency Response Team (Equipo de Respuesta ante Emergencias Informáticas).

En 1988 se produce uno de los primeros incidentes de seguridad informática a gran escala en Internet (el famoso gusano de Morris) el cual afectó a miles de sistemas conectados a la red ARPANET, demostrando de esta forma la necesidad de contar con un equipo especializado para manejar este tipo de crisis.

Como resultado, el CERT/CC (Coordination Center) fue fundado por la Universidad Carnegie Mellon en EE.UU., patrocinado por el Departamento de Defensa.

Aunque **CERT y CSIRT** (Computer Security Incident Response Team) se usan en ocasiones de forma intercambiable, **CERT** es una marca registrada por la Universidad Carnegie Mellon (CMU).

Históricamente, CMU otorgaba licencias a organizaciones, tanto dentro como fuera de Estados Unidos, para usar el término en sus nombres oficiales. Actualmente, CMU ha discontinuado la práctica de otorgar licencias internacionales para el uso de la marca "CERT". No es posible solicitar una nueva autorización para usar "CERT" en el nombre de una organización fuera de Estados Unidos, aunque CMU no se opondrá si una organización fuera de EE. UU. decide registrar una marca que incluya "CERT" en su país, pero no otorgará una licencia oficial ni el respaldo asociado.

Ref: Software Engineering Institute. (2025). Authorized Users of the CERT Mark. Carnegie Mellon University. https://insights.sei.cmu.edu/cybersecurity-center-development/authorized-users-of-the-cert-mark/

Existen otros equipos adicionales en el ecosistema de la respuesta a incidentes, sobre los cuales merece la pena hacer una mención:

PSIRT (Product Security Incident Response Team):

Un PSIRT es un equipo especializado dentro de una organización, típicamente un fabricante o proveedor de software o hardware, que se dedica a gestionar y responder a incidentes de seguridad en sus productos. Su labor incluye identificar, analizar y mitigar vulnerabilidades que puedan surgir en sus desarrollos o productos ya en uso, comunicando de manera proactiva con los clientes y usuarios sobre posibles problemas de seguridad y proporcionando actualizaciones, parches o soluciones. Muy relacionado con la actual ley de ciberresiliencia (CRA).

Desde FIRST se ha diseñado también un framework de referencia para la definición y la descripción de los servicios que rodean a un PSIRT.

ISAC (Information Sharing and Analysis Center)

Un ISAC (Information Sharing and Analysis Center) es una organización que facilita el intercambio de información y la colaboración en materia de ciberseguridad entre empresas y entidades de un mismo sector o región. Su misión principal es mejorar la protección colectiva frente a amenazas, vulnerabilidades e incidentes de seguridad que puedan afectar a la industria o área de especialización a la que pertenece.

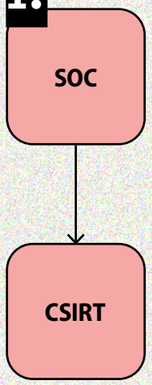
Ref: Forum of Incident Response and Security Teams. (2020). PSIRT Services Framework Version 1.1. https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1-1

Estandarización y servicios

En todas las definiciones previas realizadas hay un nexo en común, y es el hecho de que lo que define si un equipo es un SOC o un CSIRT se fija, más que por el término usado, por las funciones que este representa.

Teniendo en cuenta la labor unificadora y de estandarización de criterios a través de sus frameworks de definición, el FIRST aparece como entidad de regulación en este sentido. Siendo conscientes de esto, a través de su grupo de trabajo "CSIRT Framework Development", se desarrolla un estudio comparativo de los distintos equipos relacionados con la gestión de incidentes y las diferencias de cada uno en función de las actividades que realizan según el framework.

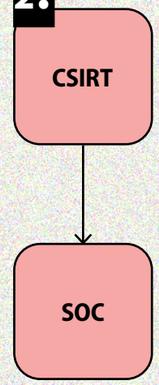
1.



El SOC se establece como equipo de alto nivel

En este modelo el CSIRT estaría formado por un equipo particular de profesionales encargados específicamente de las funciones de respuesta una vez confirmado el incidente para el SOC.

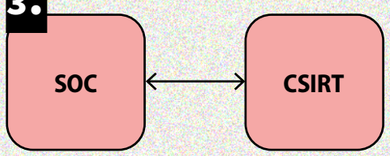
2.



El CSIRT como equipo único de alto nivel, el cual es responsable de todos los servicios y funciones

En este modelo el SOC estaría formado por un equipo particular de profesionales encargados de las funciones de monitorización y dependiendo del CSIRT.

3.

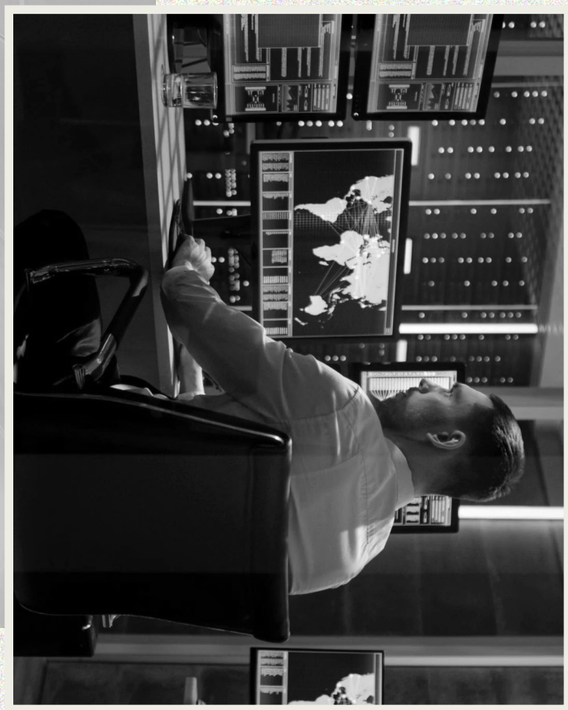


Separar los servicios teniendo en cuenta que el área de monitorización lo lleva a cabo un SOC

El SOC se encargaría de las alertas e indicios en su primer momento, trasladando al CSIRT las situaciones que superen el nivel de conocimiento y riesgo de ámbito. En este modelo el SOC y el CSIRT se encuentran al mismo nivel organizativo.

Ref: Forum of Incident Response and Security Teams. (2019). CSIRT Services Framework Version 2.1. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

EVOLUCIÓN DE LOS CENTROS DE OPERACIONES DE SEGURIDAD



4.1. INTRODUCCIÓN: LA EVOLUCIÓN DE LAS AMENAZAS Y **SU IMPACTO EN LOS SOCS**

La creación y evolución de los Centros de Operaciones de Ciberseguridad (SOC) no puede entenderse sin analizar la transformación paralela y progresiva de las amenazas de ciberseguridad a las que se enfrentan organizaciones, gobiernos y la sociedad en general. A lo largo de las últimas tres décadas, estas amenazas han evolucionado en complejidad, escala, motivación y velocidad de ejecución, forzando una respuesta igualmente sofisticada por parte de los equipos de seguridad tal y como hemos visto al inicio de este documento.

Si nos remontamos al origen del concepto del SOC, debemos volver atrás en el tiempo hasta la década de los 90. Y es que, aunque no podamos afirmarlo a ciencia cierta, probablemente el ADN original de los SOC tenga su origen en los NOC (centros de operaciones de red, por sus siglas en inglés). Los primeros SOC se crearon con el objetivo de centralizar la experiencia enfocada en la detección y respuesta. Pero, con el tiempo, su misión se ha ampliado para incluir otros aspectos que amplían las capacidades de gestión de la seguridad.

Desde entonces, la misión principal del SOC ha permanecido prácticamente igual hasta hoy en día -- detectar y responder a amenazas para proteger tu organización -- pero su ámbito de acción ha aumentado exponencialmente en alcance y complejidad. Al principio, los adversarios solían ser menos y sus ataques más esporádicos, todo lo contrario de lo que sucede actualmente.

Por esta razón, aunque la misión sigue siendo la misma, el futuro del SOC es muy diferente de lo que hemos estado operando durante las últimas décadas. Si queremos adelantarnos al desbordamiento por el crecimiento exponencial de datos, al imparable aumento del número de adversarios, a la escasez de talento y a la criticidad de los ciberataques, necesitamos evolucionar el concepto de SOC.

¿Cómo han evolucionado los SOCs para dar respuesta a cada uno de los contextos de evolución de las amenazas?

La evolución constante en el ámbito de las amenazas ha provocado una imperativa necesidad de transforma en SOC, tal y como lo conocemos actualmente; los SOCs han ido evolucionando; de lo técnico a lo estratégico, del perímetro a la visibilidad total, de la reacción a la anticipación y de la defensa a la resiliencia.

A continuación, analizaremos esta evoulción de los SOC desde su primera generación hasta los SOCs de última generación (Next Generation), pasando por conceptos mucho más complejos como los Centros de Operaciones de Ciberresiliencia (CROC).

4.2. SOCS DE **PRIMERA GENERACIÓN**

Los SOCs de primera generación surgieron en los años noventa. Su evolución estuvo marcada por un contexto de creciente digitalización en las empresas, una mayor conectividad y la aparición de amenazas cada vez de mayor escala y complejidad que exigían de una respuesta organizada y centralizada para proteger activos tecnológicos cada vez más críticos.

Los SOCs de esta generación sentaron las bases estructurales del modelo actual operación de ciberseguridad: se introdujeron tecnologías SIEM que permitieron recolectar y correlar grandes volúmenes de eventos, se desarrollaron procesos para clasificar incidentes, y se consolidó una estructura jerarquizada de analistas por niveles (N1, N2,N3).

Las capacidades técnicas de estos centros evolucionaron desde un enfoque netamente reactivo, sustentado en tecnologías como antivirus, firewalls e IDS/IPS básicos, hacia un modelo más avanzado, con cierta capacidad de análisis contextual y la incorporación de inteligencia de amenazas externa. Sin embargo, a pesar de estos avances, esta generación de SOCs mostraba aún importantes limitaciones. La escasa automatización/orquestación, la dependencia de la intervención humana, la falta de consolidación de herramientas y la limitada integración con entornos emergentes como la nube o el IoT, condicionaban su escalabilidad y eficacia ante escenarios de amenazas más complejos.

4.3. NEXT GENERATION SOCS

Los SOCs de segunda generación, comúnmente conocidos como Next Generation SOCs, surgieron como respuesta directa a un entorno de amenazas mucho más complejo y sofisticado que obligó a transformar por completo el enfoque operacional de la ciberseguridad. En este nuevo contexto, ya no era suficiente con detectar incidentes, era necesario anticiparse, conocer las amenazas específicas y agilizar las respuestas que además debían tener una precisión quirúrgica.

Los NG-SOCs se caracterizan por: su capacidad de integración avanzada de fuentes de datos de muy diversa naturaleza para dotarles de una mayor visibilidad del panorama de amenazas (entornos híbridos, endpoints, redes, aplicaciones, servicios Cloud, entornos OT, etc.); la anticipación al incidente, usando la inteligencia de amenazas estratégica y táctica junto con capacidades de Threat Hunting; la detección avanzada mediante el uso herramientas de análisis de comportamiento (UEBA) e inteligencia artificial y Machine Learning; la automatización y orquestación de las respuestas para tener una mayor eficacia y velocidad de respuesta, incorporando plataformas SOAR (Security Orchestration, Automation and Response) y el uso de inteligencia artificial (Operación Copilotada y Operación Asistida); y unas respuestas adaptadas al contexto específico de actividad de una organización mediante la especialización de los SOCs (SOCs sectoriales).

A nivel estratégico, esta generación de SOCs se orienta hacia una supervisión continua del riesgo, con visibilidad completa del panorama de amenazas específico que tiene una organización en su contexto de actividad, potenciando la fase de preparación para anticiparse a la materialización de estos riesgos y con unas capacidades avanzadas de detección, análisis y respuesta apoyándose en las nuevas capacidades que incorpora el uso de la inteligencia artificial (playbooks dinámicos, agentes virtuales) . También existe una creciente alineación de la operación de ciberseguridad con marcos normativos y regulatorios, como NIST CSF, ISO27K, ISA62443, ENS y DORA, consolidando su rol estratégico dentro de la gobernanza de la ciberseguridad corporativa.

En resumen, los Next Generation SOCs representan la evolución de una defensa reactiva, genérica y con una gran componente manual, a una defensa proactiva, avanzada, especializada y orquestada/automatizada.

Aplicación de la IA en los NG-SOCs:

La inteligencia artificial, en este contexto, se convierte en un elemento transformador de la operativa diaria los NG-SOCs, llevando a un nivel hasta ahora nunca visto las capacidades de detección, análisis y respuesta.

La detección avanzada de amenazas mediante modelos de aprendizaje automático permite analizar grandes volúmenes de datos en tiempo real, identificar anomalías complejas y generar alertas contextualizadas con una gran precisión. La Operación Copilotada (Analista humano liderando y Analista virtual ayudando) y la Operación Asistida (Analista virtual gestionando, asistido por el Analista humano) están empezando a incorporarse en las fases de análisis y respuesta ante amenazas, con la incorporación elementos disruptivos como la utilización de Playbooks dinámicos y Agentes virtuales especializados (contextualización, respuesta, análisis, etc.). Esta automatización cognitiva libera a los analistas humanos de tareas repetitivas, permitiéndoles enfocarse en actividades de mayor valor.

En un contexto donde el tiempo de respuesta es crítico, el volumen de amenazas crece exponencialmente y la naturaleza y complejidad de éstas cambia constantemente, la utilización de la inteligencia artificial se convierte en un elemento esencial de las capacidades del SOC.

Especialización sectorial de los NG-SOCs:

Asimismo, esta generación de SOCs está dando lugar en algunos escenarios a una especialización sectorial.

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener características específicas diferenciales en cada uno de los sectores, como pudieran ser entre otras:

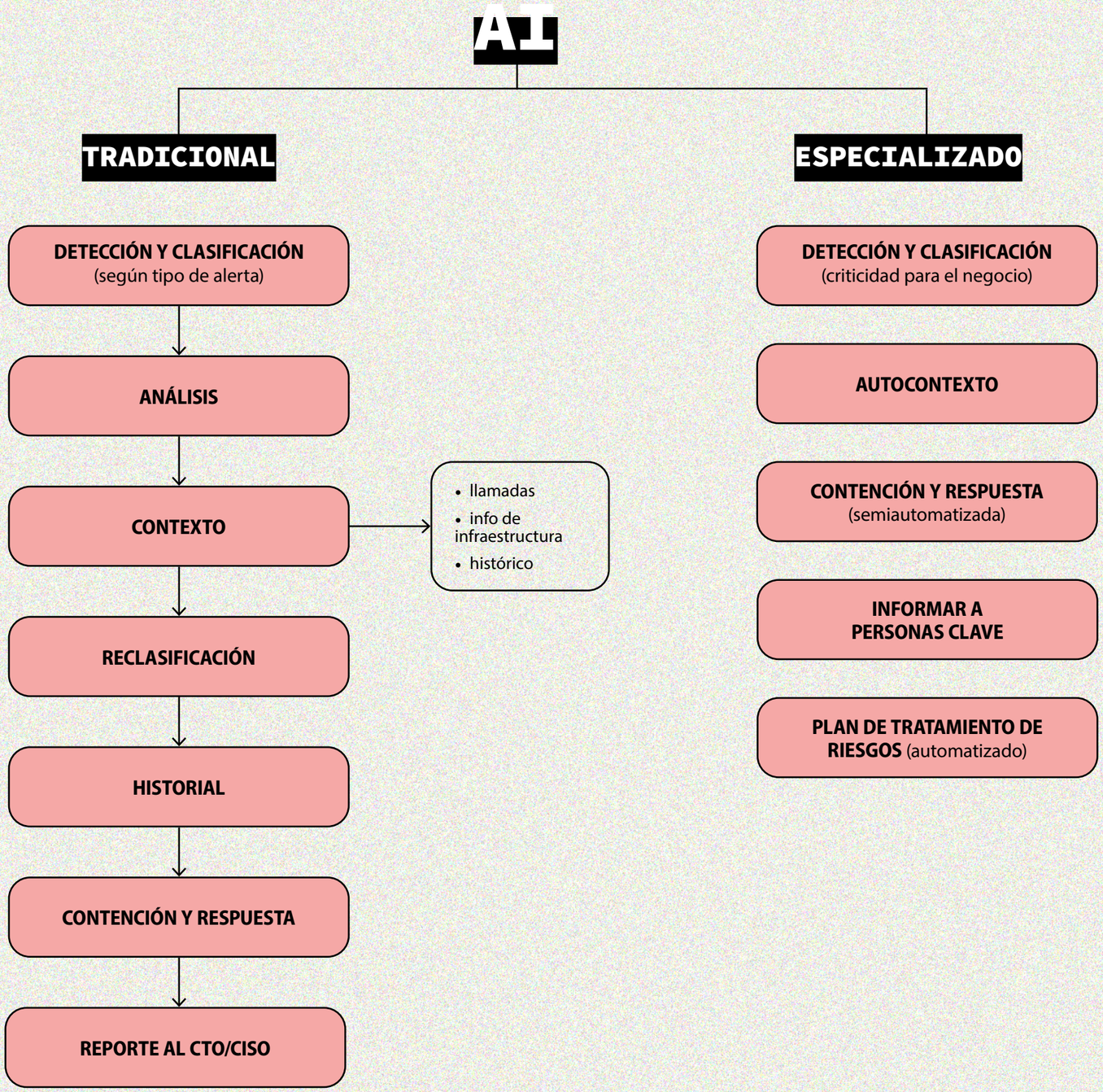
- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de la necesidad de esta especialización sectorial es que se siguen reproduciendo tipologías de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de soluciones o servicios innovadores especializados para ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Entre otras particularidades, un SOC sectorial o especializado podría incluir:

- Tecnologías específicas del sector, y casos de uso de detección especializados
- Alertas ante anomalías en los procesos de negocio específicos (p.e. integrando como fuentes de logs aplicaciones de negocio)
- Fuentes de inteligencia corporativas (habitualmente las fuentes de inteligencia que enriquecen las alertas son externas). Esto permitiría entender mejor la alerta en su contexto de negocio (criticidad, activos involucrados, procesos afectados, etc.)
- Playbooks o actuaciones ante incidentes especializadas según el sector y los activos involucrados



- Máximo contexto en cada incidencia por fuentes de inteligencia externas e internas
- SOC holístico orientado al negocio, más ráido y eficiente
- Análisis de riesgos y pan de mejora dinámicos en base a amenazas detectadas.

Ejemplo, SOC especializado en salud

El sector salud es especialmente sensible debido a la naturaleza crítica y confidencial de los datos. Un SOC especializado en salud debe contemplar:

- Monitorización de dispositivos médicos conectados (IoMT)
- Protección de historias clínicas electrónicas (EHR)
- Cumplimiento normativo (HIPAA, GDPR)
- Gestión de riesgos en entornos hospitalarios híbridos (TI + dispositivos médicos)

Como ejemplo, una red de hospitales en Europa ha desplegado un SOC especializado para detectar ataques dirigidos a sistemas de imágenes médicas (DICOM) y dispositivos IoMT. La IA ayuda a correlacionar eventos anómalos en dispositivos de resonancia magnética y conexiones de red no autorizadas, evitando una brecha crítica de datos de pacientes.

4.4.
CROC: CYBER RESILIENCE OPERATIONS CENTER

El modelo CROC representa la última evolución en el concepto de centro de operaciones de ciberseguridad, y responde a la creciente necesidad de ir más allá de la defensa técnica para garantizar la capacidad de una organización de anticiparse, resistir, recuperarse y adaptarse a amenazas e incidentes de ciberseguridad disruptivos. Los CROCs adoptan una visión integral de seguridad, continuidad de negocio y cultura organizacional resiliente.

En un contexto donde los ataques son cada vez más complejos, persistentes y con impactos que afectan al negocio en su conjunto, los CROC se configuran como centros multidisciplinares que integran capacidades técnicas, organizativas y estratégicas.

Los CROC no se limitan a la detección y respuesta tradicional, sino que también gestionan la preparación ante crisis, la recuperación tras incidentes y la coordinación transversal entre áreas de una organización, como las áreas de tecnología, legal, comunicación, compliance y dirección ejecutiva. Su enfoque está alineado con marcos normativos y estratégicos como NIST SP 800-160, DORA y ENS.

Desde el punto de vista tecnológico, estos centros integran capacidades avanzadas de automatización, telemetría extendida, simulación de crisis, análisis forense en tiempo real y gestión continua del riesgo. El CROC se convierte así en una unidad clave para garantizar la resiliencia digital de una organización, con enfoque preventivo, adaptativo y orientado a la recuperación efectiva.

El papel de la inteligencia artificial en la ciberresiliencia es clave para mejorar entre otras las capacidades de: simulación y planificación de escenarios de crisis, mediante modelos predictivos; análisis en tiempo real impacto de riesgos, automatización de procesos de recuperación basados en IA contextual y el apoyo en la toma de decisiones estratégicas mediante Dashboards de resiliencia organizacional.

CAPACIDADES TIPOS DE SOC

Capacidad	SOC de 1ª generación	Next Generation SOC	CROC
Preparación	Baja	Alta	Óptima
Detección	Media	Alta	Alta
Análisis	Media	Alta	Alta
Contención	Baja	Media	Alta
Erradicación	Baja	Media	Alta
Recuperación	Baja	Media	Óptima
Automatización	Mínima	Alta	Óptima
Orquestación	Inexistente	Media	Alta
Inteligencia de amenazas	Baja	Alta	Óptima

05

MODELOS DE DESPLIEGUE DE UN SOC

5.1. CONCEPTOS. **TIPOS DE SOC.**

A nivel general, podemos clasificar los SOC desde dos ejes :

- Organizacion corporativa y operación
- Entorno a proteger

Atendiendo a la Organización corporativa y la operación, podemos dividirlos en:

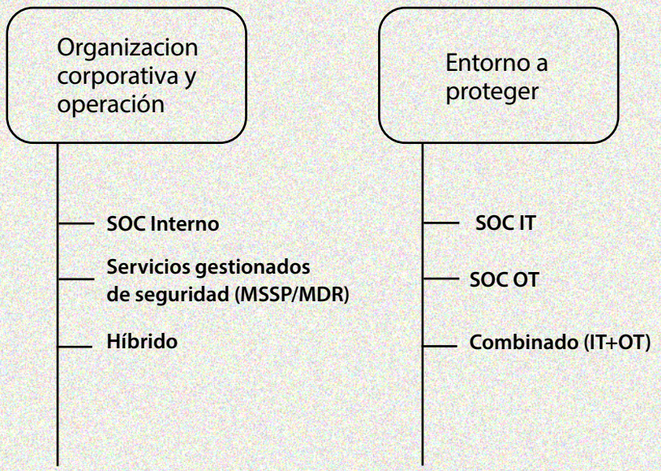
- SOC Interno
- Servicios gestionados de seguridad (MSSP/MDR)
- Hibrido

Desde el punto de vista del entorno a proteger;

- SOC IT
- SOC OT
- Combinado (IT + OT)

Los modelos de despliegue para un servicio de Centro de Operaciones de Seguridad (SOC) determinan cómo se estructura, quién lo opera y cómo se entregan los servicios de seguridad.

TIPOS DE SOC.



SOC Interno

En este modelo organizativo de un Centro de operaciones de Seguridad, es la organización/corporación quien diseña, implementa, gestiona y opera su propio SOC utilizando personal, tecnología y procesos internos. El "servicio" de SOC se provee desde un departamento interno al resto de la organización.Como puntos positivos en este modelo se destaca lo siguiente:

Control Total: La empresa tiene el máximo control sobre los datos, las herramientas, los procesos y las prioridades.

Personalización: Se puede adaptar completamente a las necesidades y al contexto específico del negocio.

Conocimiento Interno: El equipo posee un conocimiento profundo del entorno y los activos críticos.

Por el contrario, este modelo también tiene sus puntos menos adecuados para una organización entre los que cabría destacar estos:

Coste Elevado: Requiere una inversión significativa en personal especializado (difícil de contratar y retener), tecnología (SIEM, SOAR, EDR, etc.) y formación continua, tanto en adquisición como en su mantenimiento posterior.

Complejidad de Implementación: Ponerlo en marcha y mantenerlo operativo 24/7 es un desafío considerable. La alta rotación de personal también lo hace complejo a la hora de mantener este modelo.

Un modelo de SOC interno podemos indicar como servicio mas adecuado para organizaciones grandes, con alta madurez en seguridad, requisitos regulatorios estrictos que exigen control total de datos, y con recursos financieros y humanos para que sea sostenible en el tiempo.

Servicios gestionados de Seguridad (MSSP/MDR)

Dentro de los servicios gestionados de SOC de seguridad encontramos dos modelos diferenciados, SOC Externalizado a través de un MSSP (Managed Security Service Provider) y SOC Externalizado a través de un MDR (Managed Detection and Response).

SOC Externalizado a través de un MSSP (Managed Security Service Provider)

Descripción del Servicio: Se contrata a un proveedor externo (MSSP) para que entregue un conjunto de servicios de seguridad. Esto es un modelo de "SOC-as-a-Service" donde el MSSP utiliza su propia infraestructura y personal para servir a múltiples clientes.

Características Clave y aspectos positivos:

- **Monitorización y Alertas:** Principalmente enfocado en la monitorización de seguridad (logs, eventos), gestión de dispositivos (firewalls, IDS/IPS) y generación de alertas.
- **Cobertura 24/7:** Suelen ofrecer monitorización continua.
- **Coste (OpEx):** Modelo de gasto operativo, potencialmente más predecible y menor que un SOC interno completo para servicios básicos.

Aspectos menos beneficiosos para las organizaciones:

- **Expertise Externo:** Acceso a un pool de profesionales de seguridad del proveedor. La falta de expertise interno puede afectar en los modelos de análisis y tiempos de respuesta junto con la limitación del conocimiento del entorno y los activos críticos de la compañía.
- **Menor Control Directo:** La personalización puede ser limitada y los procesos son los del proveedor.
- **Enfoque en Notificación:** Tradicionalmente, los MSSP notifican al cliente sobre las alertas, y el cliente a menudo es responsable de la investigación profunda y la remediación. (Esto está evolucionando en algunos MSSP).

Consideramos que este modelo puede ser ideal para organizaciones con un nivel bajo o medio de madurez, que no cuentan con las capacidades necesarias a nivel de recursos internos y necesitan cumplir con requisitos de monitorización, buscan una cobertura 24/7 básica, tienen presupuestos limitados para un SOC interno completo, o desean externalizar la gestión de la seguridad.

SOC Externalizado a través de un MDR (Managed Detection and Response)

Descripción del Servicio: Se trata de un tipo especializado de "SOC-as-a-Service" que se enfoca en la monitorización y detección de amenazas, la caza de amenazas (threat hunting) y, fundamentalmente, la respuesta a los incidentes.

Características Clave y aspectos positivos:

- **Detección y Respuesta:** Va más allá de las alertas, incluyendo la investigación profunda y la ayuda activa en la contención y remediación.
- **Tecnología Avanzada:** Suelen emplear y gestionar tecnologías como EDR (Endpoint Detection and Response), XDR (Extended Detection and Response) y plataformas de inteligencia de amenazas.
- **Expertise Especializado:** Cuentan con todos los niveles de analistas y respuesta ante incidentes.
- **Proactividad:** Incluye el servicio de threat hunting.

Desafíos para las organizaciones dentro de este modelo:

- **Coste (OpEx):** Generalmente más elevado que un MSSP básico debido a la mayor especialización y el componente de respuesta.
- **Conocimiento interno limitado:** Al igual que en el modelo MSSP el conocimiento del entorno y los activos críticos de la compañía es limitado lo que puede afectar en los modelos de análisis y respuesta.

Consideramos que este modelo puede ser ideal para organizaciones de cualquier tamaño que necesiten capacidades avanzadas de detección y respuesta que no pueden desarrollar internamente, o que quieran mejorar sus capacidades actuales de MSSPs.

Estos dos modelos de servicios externalizados pueden encajarse junto con un modelo interno lo que lleva a otro modelo de SOC que sería el SOC Híbrido, donde la organización mantiene un equipo de seguridad interno que colabora con un proveedor externo para mantener el servicio de forma conjunta.

SOC Híbrido

En un entorno hibrido, se combinan las características de un SOC interno con un MSSP. Generalmente la infraestructura tecnológica y los datos se mantienen dentro de la corporación y se usan los servicios MSSP de una o varias empresas externas para operar y evolucionar la plataforma.

Características Clave y aspectos positivos:

- **Combinación de Fortalezas:** Se busca el control y conocimiento interno en áreas estratégicas, complementado con la eficiencia, cobertura 24/7 o especialización del proveedor externo.
- **Flexibilidad:** Permite externalizar funciones específicas (ej. monitorización nocturna, caza de amenazas, gestión de EDR) mientras se retienen otras internamente.
- **Optimización de Recursos:** El equipo interno puede centrarse en tareas de mayor valor estratégico, mientras el proveedor maneja operaciones más rutinarias o especializadas.

Como **desafíos para las organizaciones** en este modelo destacamos:

- Complejidad de Coordinación: Requiere una clara definición de roles, responsabilidades, elaboraciones de indicadores para la valoración y seguimiento del servicio. También será fundamental una comunicación fluida entre el equipo interno y el proveedor.

Consideramos este modelo híbrido como ideal para organizaciones que ya tienen alguna capacidad de seguridad interna pero necesitan aumentarla, especializarla, obtener cobertura 24/7, o gestionar picos de trabajo sin contratar personal adicional permanente.

SOC IT

Es el mas común. Generalmente, cuando hablamos de SOC nos referimos a SOC IT. Son los SOC que protegen el entorno IT: aplicaciones, frontend, backend, servicios web, bases de datos, microservicios, etc

SOC OT

Un SOC OT *(Operational Technology Security Operations Center)* es un centro de operaciones de seguridad especializado, con personal, procesos y tecnología específicamente diseñados para monitorizar, detectar y responder a incidentes de ciberseguridad en entornos de Tecnología Operacional.

Un SOC OT se centra en proteger los **Sistemas de Control Industrial (ICS)**, que gestionan procesos físicos. Esto incluye sistemas como SCADA, PLCs (Controladores Lógicos Programables), y DCS (Sistemas de Control Distribuido). También se considera OT la infraestructura de red de una TELCO (equipos especializados de radio, transporte o core).

El objetivo principal de un SOC OT no es solo proteger datos, sino **garantizar la seguridad, la disponibilidad y la integridad de los procesos industriales,** previniendo interrupciones operativas, daños físicos a la maquinaria, desastres medioambientales o riesgos para la vida humana.

El servicio SOC OT tiene las siguientes características esenciales adaptadas al mundo industrial:

- **Personal híbrido,** no sólo experto en ciberseguridad sino que también entienda procesos industriales, ingeniería de control y protocolos OT.
- **Colaboración IT/OT:** Es fundamental una colaboración estrecha entre el equipo de seguridad (IT) y los ingenieros de planta (OT), que son quienes realmente entienden el estado normal del proceso.
- **Monitorización Pasiva:** La monitorización debe ser no intrusiva para no afectar a los sistemas de control. Se utilizan sensores de red que escuchan el tráfico sin interactuar activamente.

- **Playbooks de Respuesta OT:** Los planes de respuesta a incidentes deben estar predefinidos, probados y aprobados por los ingenieros de planta. Deben considerar el impacto físico de cada acción.
- **Gestión de Vulnerabilidades Basada en Riesgo:** Se enfoca en la segmentación de red, el control de accesos y la implementación de controles compensatorios.
- **Gestión de Activos:** un paso necesario es tener un inventario completo y preciso de todos los dispositivos a nivel IT/ OT, sus versiones de firmware y cómo se comunican.
- **Plataformas de Monitorización de Red OT/ICS:** Herramientas especializadas que puedan decodificar protocolos industriales, identificar activos y detectar amenazas específicas de OT.
- **SIEM con Contexto OT:** Un SIEM que pueda ingerir y entender logs de fuentes OT y correlacionarlos con eventos de TI. Debe tener reglas de correlación específicas para ataques a ICS.
- **Soluciones de Acceso Remoto Seguro:** Herramientas para gestionar y monitorizar el acceso de personal interno y de terceros (proveedores) a la red OT.

Principales desafíos en este modelo de gestión:

- **Convergencia IT/OT:** La conexión creciente de las redes industriales a las redes corporativas para mejorar la eficiencia ha abierto nuevas vías de ataque.
- **Sistemas Legacy:** La larga vida útil de los equipos de OT significa que muchos son antiguos, no tienen parches y carecen de funciones de seguridad básicas.
- **Escasez de Talento:** Faltan profesionales que tengan un conocimiento profundo tanto de ciberseguridad como de tecnología operacional.
- **Cultura Organizacional:** Superar la brecha cultural e histórica entre los equipos de TI y de OT, que tradicionalmente han operado en silos con prioridades diferentes.

Combinado IT/OT

Hay una tendencia creciente a combinar en un solo SOC la monitorización de los entornos IT y OT, aunando esfuerzos y promoviendo sinergias. En este modelo cada entorno tiene sus sensores, y ambos vuelcan sus eventos a un unico SIEM combinado que genera alertas tanto de un entorno como de otro. Generalmente los procedimientos de gestion de los incidentes son distintos en un entorno IT que en OT, tanto en procedimiento como en personal involucrado.

5.2. CLASIFICACIÓN DE SERVICIOS DE **CIBERSEGURIDAD.**

En esta guía queremos presentar un modelo para clasificar los servicios de ciberseguridad en tres niveles de madurez: Esencial, Avanzada y Resiliente. El objetivo es tratar de ayudar a que las organizaciones, independientemente de su tamaño o sector, puedan evaluar sus capacidades actuales y planificar la evolución de su estrategia de seguridad.

El modelo se estructura en torno a cinco funciones fundamentales, alineadas con los marcos de ciberseguridad más reconocidos (como el de NIST): Identificación, protección, monitorización/detección, respuesta y gobierno, con su nivel de servicio:

- **Servicios Esenciales:** Imprescindibles para la operación y seguridad del día a día.
- **Servicios Gestionados Avanzados:** Servicios que van más allá de lo esencial buscando a nivel superior en el medio largo plazo. Enfatiza la mejora de la eficiencia, velocidad y eficacia en los servicios implantados.
- **Servicios de Transformación y Resiliencia:** El objetivo es que las organizaciones estén preparadas para el futuro, permitiéndolas no solo resistir a las adversidades (Resiliencia) sino también liderar el cambio (Transformación).

Podemos visualizar este modelo como un radar de madurez, donde cada eje representa una función. Una organización madura tendrá un radar más expandido y equilibrado.

Detalle de Servicios por Función y Nivel

A continuación, se detallan los servicios específicos para cada función y nivel de madurez.

1. Identificación

Objetivo: Conocer qué hay que proteger y por qué. El objetivo es identificar los activos tecnológicos, las dimensiones más relevantes de los mismos a nivel de ciberseguridad, el contenido a nivel de activo de información y su estatus.

NIVEL	SERVICIO /SOLUCIÓN	DESCRIPCIÓN
ESENCIAL	INVENTARIO DE ACTIVOS (MANUAL)	MANTENER UN REGISTRO BÁSICO (EJ. EN UNA HOJA DE CÁLCULO) DE LOS ACTIVOS DE HARDWARE Y SOFTWARE CRÍTICOS.
	ESCANEO DE VULNERABILIDADES BÁSICO	REALIZAR ESCANEOS PERIÓDICOS PARA IDENTIFICAR LAS VULNERABILIDADES MÁS COMUNES Y CONOCIDAS EN LOS SISTEMAS.
AVANZADO	DESCUBRIMIENTO Y GESTIÓN AUTOMATIZADA DE ACTIVOS	UTILIZAR HERRAMIENTAS QUE DESCUBREN Y MANTIENEN AUTOMÁTICAMENTE UN INVENTARIO DE TODOS LOS DISPOSITIVOS CONECTADOS A LA RED.
	GESTIÓN CONTEXTUALIZADA DE VULNERABILIDADES	NO SOLO ESCANEAR, SINO PRIORIZAR LAS VULNERABILIDADES BASÁNDOSE EN LA CRITICIDAD DEL ACTIVO Y LA INTELIGENCIA DE AMENAZAS.
	GESTIÓN DE POSTURA DE SEGURIDAD CLOUD (CSPM/SSPM)	EVALUAR CONTINUAMENTE LAS CONFIGURACIONES DE SEGURIDAD DE LAS PLATAFORMAS CLOUD (IAAS/SAAS) PARA DETECTAR ERRORES.
RESILIENTE	GESTIÓN DE LA SUPERFICIE DE ATAQUE (ASM)	IDENTIFICAR Y ANALIZAR CONTINUAMENTE TODOS LOS ACTIVOS EXPUESTOS A INTERNET (CONOCIDOS Y DESCONOCIDOS) DESDE LA PERSPECTIVA DE UN ATACANTE.
	EJERCICIOS DE RED TEAM	SIMULAR ATAQUES PARA PROBAR DE FORMA PRÁCTICA LA EFECTIVIDAD DE LOS CONTROLES DE SEGURIDAD Y LA RESPUESTA.

2. Protección

Objetivo: Desarrollar e implementar las protecciones apropiadas para asegurar la entrega de servicios críticos e importantes y limitar el impacto de un evento de ciberseguridad.

NIVEL	SERVICIO /SOLUCIÓN	DESCRIPCIÓN
ESENCIAL	ANTIVIRUS / ANTIMALWARE	Proteger los endpoints contra malware conocido y variantes comunes mediante firmas proporcionadas por los fabricantes.
	FIREWALL PERIMETRAL Y DE HOST	Filtrar el tráfico de red no deseado en el borde de la red y en los propios dispositivos.
	AUTENTICACIÓN Y GESTIÓN DE CREDENCIALES	Aplicar políticas de contraseñas seguras y establecer una norma de cambio de credenciales periódico.
	DELIMITACIÓN DE ACCESOS A SERVICIOS INTERNOS	Control de acceso a red interna a través de servicios VPN para delimitar los accesos y garantizar un mínimo privilegio en los accesos a sistemas corporativos.
	BACKUPS	Realizar copias de seguridad periódicas de los datos críticos.
AVANZADO	PROTECCIÓN DEL ENDPOINT	Endpoint Detection and Response (EDR)Obtener visibilidad profunda y capacidad de respuesta en los endpoints para detectar y contener amenazas avanzadas. Servicios avanzados de protección de red interna incluyeno MFA como segundo factor de verificación a sistemas.
	PROTECCIÓN DE NAVEGACIÓN	Servicios de control de navegación que permitan asegurar el tráfico de los dispositivos corporativos y garantizar las políticas de seguridad establecidas en el acceso hacia Internet.
	GESTIÓN CONTEXTUALIZADA DE VULNERABILIDADES	No solo escanear, sino priorizar las vulnerabilidades basándose en la criticidad del activo y la inteligencia de amenazas.
	PROTECCIÓN DE CORREO ELECTRÓNICO	Filtrar phishing, malware y spam con técnicas avanzadas como eliminación proactiva de correos sospechosos, activación de protección específica de correo: DKIM, SPF y DMARC, inspección avanzada de adjuntos y análisis de códigos QR embebidos
	SEGMENTACIÓN DE RED	Dividir la red en zonas para limitar la propagación lateral de un atacante.
	WEB APPLICATION FIREWALL (WAF)	Proporcionar protección a las aplicaciones web y APIs frente a ataques externos.
RESILIENTE	CLOUD ACCESS SECURITY BROKER (CASB). ARQUITECTURA ZERO TRUST	Intermediar el acceso entre los usuarios y los servicios en la nube para aplicar políticas de seguridad y protección de datos. Aplicar el principio de ***"nunca confiar, siempre verificar"*** para todos los accesos, independientemente de la ubicación.
	PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)	Implementar políticas granulares para detectar y prevenir la exfiltración de datos sensibles.
	GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESOS	Garantizar los accesos a través de herramientas de ***Gestión de Identidades*** y establecer políticas para garantizar el acceso de mínimo privilegio a los aplicativos internos.

3. Monitorización y Detección

Objetivo: Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad de manera oportuna.

NIVEL	SERVICIO /SOLUCIÓN	DESCRIPCIÓN
ESENCIAL	GESTIÓN Y MONITORIZACIÓN DE LOGS	Centralizar y revisar logs de sistemas críticos (firewalls, servidores, protección de endpoints) para detectar anomalías.
	ALERTAS DE SEGURIDAD BÁSICAS	Configurar alertas automáticas para eventos de seguridad de alta prioridad (ej. múltiples fallos de inicio de sesión).
AVANZADO	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	Correlacionar eventos de múltiples fuentes en tiempo real para detectar patrones de ataque complejos. Dentro de esta correlación es fundamental una mejora continua en los Casos de Uso para que la monitorización sea lo más precisa y avanzada posible. Los servicios de SOC MSSP/MDR deben ofrecer servicios de almacenamiento/retención adecuadas para las compañías así como reporting continuo adaptado a las necesidades.
	MONITORIZACIÓN DE SEGURIDAD CLOUD	Ingestar y analizar logs de proveedores de nube (AWS, Azure, Google Cloud) para detectar amenazas específicas.
	INTELIGENCIA DE AMENAZAS (THREAT INTEL)	Integrar feeds de Indicadores de Compromiso (IOCs) para detectar amenazas conocidas en los sistemas de las compañías. Los feeds también pueden ayudar al servicio de Gestión de vulnerabilidades para responder ante nuevas amenazas no parcheadas en los servicios internos de las compañías.
RESILIENTE	EXTENDED DETECTION AND RESPONSE (XDR)	Plataforma unificada que correlaciona datos de endpoints, red, nube e identidad para una detección y respuesta holística.
	CAZA PROACTIVA DE AMENAZAS (THREAT HUNTING)	Búsqueda activa y dirigida por hipótesis de amenazas que han eludido las defensas automatizadas, realizada por analistas expertos. Este servicio puede ser ofrecido por los servicios gestionados como añadido a Threat Intel.
	TECNOLOGÍAS DE ENGAÑO	Desplegar señuelos (honeypots, credenciales falsas) para detectar, analizar y desviar a los atacantes.

4. Respuesta

Objetivo: Desarrollar e implementar las actividades apropiadas para tomar acción respecto a un evento de ciberseguridad detectado.

Nivel	Servicio/Solución	Descripción
ESENCIAL	Plan de respuesta a incidentes	Disponer de un documento que define los pasos básicos, roles y contactos en caso de un incidente de seguridad. Soporte de servicio externo + Playbooks básicos de respuesta.
AVANZADO	Servicio de Respuesta a incidentes	**Playbooks avanzados de Respuesta:** Guías detalladas y paso a paso para gestionar tipos específicos de incidentes (ej. ransomware, phishing). **Orquestación y Automatización (SOAR):** Utilizar tecnología para automatizar tareas repetitivas de respuesta a incidentes, como enriquecer alertas o bloquear IOCs. **Respuesta alternativa:** Tener servicios de respuesta masiva alternativos para poder responder de forma más rápida en caso de incidente.
	Respuesta Gestionada (MDR Service)	Contratar un servicio externo que no solo detecta, sino que también toma acciones de contención en nombre de la organización así como ayuda internamente en la mejora continua de la fase de detección/monitorización proponiendo o mejorando los Casos de Uso ya existentes. Se trata que en un concepto de SOC híbrido, las compañías puedan trabajan en un concepto de mejora continua del servicio de monitorización junto son el Servicio Gestionado.
RESILIENTE	Retainer de Respuesta a Incidentes y Forense (DFIR)	Tener un contrato con una firma experta para una respuesta rápida y profunda ante incidentes graves, incluyendo análisis forense.
	Ingeniería Inversa de Malware	Análisis del código malicioso para determinar sus capacidades, indicadores de compromiso (IoCs) y objetivos
	Correlación con Inteligencia de Amenazas	Vinculación de la evidencia encontrada con actores de amenaza conocidos y sus TTPs (mapeo con frameworks como MITRE ATT&CK)
	Simulaciones de Incidentes a Escala Real	Realizar simulaciones con el IRT + áreas de IT implicadas en caso de incidente IT + simulaciones especializadas con la organización (legal, comunicación, dirección).

5.3. ESTRUCTURA DE NIVELES EN **SERVICIOS SOC.**

Un pilar fundamental de los servicios de SOC, ya sean internos, gestionados o híbridos, es la estructuración en niveles (Tiers) según la capacidad técnica y la experiencia de los analistas. Esta jerarquía asegura que las alertas de seguridad sean tratadas por el personal adecuado en el momento oportuno.

Nivel 1 (L1): La Primera Línea de Defensa. Los analistas de Nivel 1 son los encargados de la monitorización continua de los sistemas, la detección inicial de incidentes y el triaje de alertas. Sus responsabilidades principales incluyen la identificación de amenazas conocidas, el descarte de falsos positivos y la escalada de incidentes que requieren un análisis más profundo. En un modelo de SOC gestionado, estas tareas suelen ser operativizadas por el proveedor del servicio, que cuenta con la infraestructura y el personal para ofrecer una cobertura 24/7 de manera costo-efectiva.

Nivel 2 (L2): Análisis y contención. Cuando un incidente es escalado por el Nivel 1, los analistas de Nivel 2 entran en acción. Este equipo posee una mayor experiencia y conocimientos para llevar a cabo investigaciones más complejas, analizar el malware, correlacionar eventos de distintas fuentes y coordinar la respuesta al incidente. Aquí es donde el modelo híbrido demuestra su gran valor.

Nivel 3 (L3): Analisis avanzado de incidentes. Es la capa mas experta y avanzada dentro de la operación. Estan especializados en tecnologías, y con grados altos de certificación y competencia. Realizan taras de análisis avanzado de incidentes, Threat Hunting proactivo y diseño de soluciones avanzadas.

5.4. EL ROL CLAVE DEL **“IMPLANT”** EN EL SOC HÍBRIDO.

El término implant se refiere a un experto del proveedor de servicios gestionados que trabaja físicamente en las instalaciones del cliente. En el contexto de un SOC híbrido, es común que una compañía acuerde con su proveedor que los servicios de Nivel 1 sean gestionados de forma remota, mientras que las responsabilidades de Nivel 2 y 3 sean asumidas por uno o varios de estos analistas implantados.

Esta configuración ofrece ventajas significativas:

- **Servicio Dedicado y Personalizado:** A diferencia de un analista de Nivel 2 que trabaja de forma remota para múltiples clientes, el implant se dedica en exclusiva a la organización en la que está asignado. Esto permite una atención focalizada y una respuesta más rápida a los incidentes.
- **Conocimiento Profundo de los Activos:** Al estar inmerso en el día a día de la compañía, el analista implantado adquiere un conocimiento detallado y contextual de los activos críticos, la arquitectura de red, las aplicaciones de negocio y las particularidades operativas. Esta comprensión es crucial para una investigación de incidentes más eficaz y para la identificación de amenazas que podrían pasar desapercibidas para un analista externo.
- **Mejora en la Comunicación y Colaboración:** La presencia física del analista de Nivel 2 facilita una comunicación fluida y directa con los equipos internos de TI, seguridad y negocio. Esto agiliza la recopilación de información, la toma de decisiones y la implementación de medidas de contención y remediación.
- **Transferencia de Conocimiento:** La interacción constante entre el implant y el personal interno fomenta una valiosa transferencia de conocimientos, contribuyendo a elevar la madurez en ciberseguridad de la propia organización.

Este servicio de implant también puede ofrecer a las organizaciones complementar el servicio de Nivel 1 externalizado con N1 que se alojen en la infraestructura del cliente y se apoyan en el expertise interno para compartir conocimiento. De esta forma, las organizaciones forman en el conocimiento de activos internos y los N1 adquieren una formación específica que, con el paso del tiempo, es muy útil para la organización que adquiere este servicio.

De esta forma se consigue una relación mucho más cercana con el N1 mientras se va adquiriendo conocimiento interno lo que da como resultado sinergias muy positivas en el modelo híbrido de SOC y, económicamente, es óptimo para las organizaciones puesto el gasto es mejor comparativa a analistas N2.

En definitiva, el modelo híbrido de SOC, con la incorporación de implants en cualquiera de los niveles 1 o 2, ofrece un equilibrio estratégico. Las empresas se benefician de la eficiencia y la cobertura ininterrumpida de un servicio gestionado para el triaje inicial de alertas, al tiempo que aseguran un análisis y una respuesta a incidentes de alto nivel, profundamente contextualizados y alineados con las especificidades de su negocio.

5.5. **ACUERDOS** DE NIVEL DE SERVICIO

Las compañías que contraten servicios gestionados de ciberseguridad (MSSP/MDR) deben tener en cuenta que los Acuerdos de Nivel de Servicio (SLAs) no son mera burocracia contractual; son el pilar que define la eficacia y fiabilidad del servicio. Un SLA es la promesa cuantificable y exigible de un proveedor, que traduce sus capacidades en compromisos de tiempo y acción.

Los SLAs son la principal herramienta para medir el rendimiento, asegurar la rendición de cuentas y garantizar que recibe la protección por la que paga.

Diferencia Clave en los SLAs: MSSP vs. MDR

Aunque a menudo se ofrecen juntos, el foco de los SLAs difiere:

- **SLAs de MSSP:** Tradicionalmente, se centran en la gestión y disponibilidad. Sus SLAs típicos incluyen el tiempo de actividad de los dispositivos gestionados (firewalls, etc.), la disponibilidad de la plataforma de monitorización y los tiempos de notificación de alertas.
- **SLAs de MDR (Detección y Respuesta Gestionada):** Son mucho más críticos y se centran en la velocidad y efectividad de la respuesta a amenazas. El tiempo es el factor esencial, y los SLAs deben reflejar esa urgencia.

Los SLAs Fundamentales en MDR

Al evaluar un proveedor de MDR, estos son los SLAs basados en tiempo que marcan la diferencia entre un servicio promedio y uno de élite. Deben estar claramente definidos, medirse 24/7/365 y tener penalizaciones asociadas por incumplimiento.

1. Tiempo Medio de Acuse de Recibo (TTA - Time to Acknowledge)

- ¿Qué es? El tiempo máximo que transcurre desde que se genera una alerta crítica hasta que un analista humano la asigna para su investigación.
- ¿Por qué es importante? Es la primera garantía de que la alerta no ha caído en un vacío. Un TTA bajo demuestra que el proveedor tiene personal activo monitorizando y no depende únicamente de notificaciones automáticas.
- ¿Qué buscar?
  - Excelente: < 15 minutos.
  - Bueno: 15-30 minutos.
  - Aceptable: < 1 hora.

2. Tiempo Medio de Triaje/Investigación (MTTI - Mean Time to Investigate)

- ¿Qué es? El tiempo que tarda un analista en investigar la alerta acusada, enriquecerla con contexto, descartar si es un falso positivo y confirmar si se trata de un incidente de seguridad real.
- ¿Por qué es importante? Mide la eficiencia del equipo de analistas. Un MTTI bajo significa que el proveedor puede diferenciar rápidamente el ruido de las amenazas reales, permitiendo concentrar los esfuerzos donde realmente importa.
- ¿Qué buscar? Este SLA suele estar integrado en el de respuesta, pero si se desglosa, un objetivo de < 60 minutos para alertas críticas es un indicador de madurez.

3. Tiempo Medio de Respuesta/Contención (MTTR/MTTC - Mean Time to Respond/Contain)

- ¿Qué es? Este es el SLA más crítico de este servicio. Mide el tiempo que transcurre desde que se confirma un incidente hasta que el proveedor toma la primera acción de contención activa para detener la propagación de la amenaza.
- ¿Qué significa "Respuesta/Contención"? No es la solución completa del problema. Es la acción inmediata para "detener la hemorragia". Ejemplos:
  - Aislar un endpoint comprometido de la red.
  - Deshabilitar una cuenta de usuario vulnerada.
  - Bloquear una dirección IP maliciosa en el firewall.
- ¿Por qué es importante? Cada segundo que un atacante tiene acceso sin restricciones aumenta el daño potencial exponencialmente. Este SLA es el verdadero indicador de la capacidad de respuesta de un proveedor.
- ¿Qué buscar?
  - Excelente: Contención remota en < 1 hora para incidentes críticos.
  - Bueno: < 2 horas.

4. Tiempo Medio de Remediación (MTTR - Mean Time to Remediate)

- ¿Qué es? El tiempo que se tarda en erradicar por completo la amenaza del entorno (eliminar malware, backdoors, etc.) y restaurar los sistemas a su estado normal.
- Es muy poco común que un proveedor de MDR ofrezca un SLA estricto para la remediación completa. La razón es que la remediación a menudo depende de la colaboración y las acciones del equipo de TI del cliente (reinstalar sistemas, restaurar backups, etc.).
- ¿Qué buscar? En lugar de un SLA de tiempo, busca un compromiso de proporcionar un **Plan de Remediación** detallado en un plazo definido (ej. 24 horas) tras la contención.

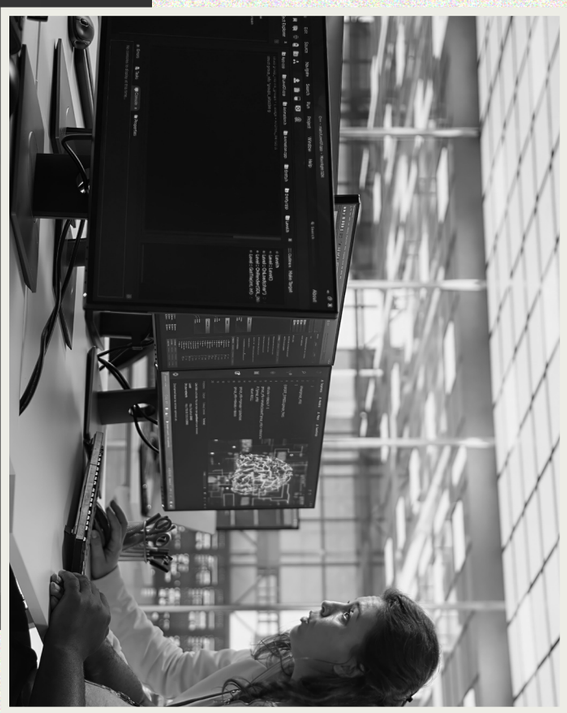
5.6. PUNTOS CLAVE PARA LA EVALUACIÓN DE **SERVICIOS MSSP/MDR**

- **Modelo de colaboración:** ¿Cómo se integra el proveedor con el equipo interno en un modelo de SOC Híbrido?
- **Transparencia y visibilidad:** Permitir accesos a datos brutos, realización de informes y dashboards que permitan visibilizar la estructura monitorizada. Testeo de calidad de las reglas por una compañía independiente.
- **Capacidades de integración:** Las herramientas y procesos existentes del cliente deben poder ser integradas por parte del servicio al que se pretenda evaluar.
- **Experiencia y verticalización:** Comprobar que el proveedor tiene experiencia en el sector del cliente que lo quiera contratar.
- **Cobertura Horaria:** ¿El servicio de análisis y respuesta es realmente 24/7/365 con analistas humanos "follow the sun" o depende de la automatización fuera del horario laboral?
- **Claridad en los SLA'S** (Acuerdos de nivel de servicio): Tiempos de detección, respuesta y notificación.
  - Tiempo Medio de Detección (MTTD): ¿Cuánto tardan en detectar una amenaza real?
  - Tiempo Medio de Respuesta (MTTR): ¿Cuánto tardan en tomar una acción de contención?
  - Tiempo de Notificación: ¿Cuánto tardan en informarte de un incidente crítico?
- **Experiencia y Certificaciones:** ¿Qué nivel de experiencia y certificaciones (GIAC, SANS, OSCP, etc.) tienen sus analistas (Nivel 1, 2, 3)?
- **Modelo de Interacción:** ¿Tendrás acceso directo a los analistas que investigan tus incidentes o solo a un gestor de cuentas? Una comunicación fluida con los expertos es clave durante una crisis.

5.7. CONCLUSIÓN

Los distintos modelos de SOC son un modelo de mejora continua y sirve como hoja de ruta para ayudar a las organizaciones a navegar ese viaje, permitiéndoles tomar decisiones informadas sobre dónde invertir sus recursos para reducir el riesgo de manera efectiva y construir una postura de seguridad resiliente. La elección correcta no tiene por qué ser la más barata, sino la que se pueda convertir en una extensión de confianza equipo de ciberseguridad, aportando la experiencia y la capacidad de respuesta necesaria para defender a las organizaciones.

PLAN DE PROYECTO



6.1. SOC COMO PARTE DEL **ROADMAP DE SEGURIDAD**

Hemos visto en capítulos anteriores que la figura del CISO, responsable principal de la estrategia de seguridad, ha de definir, dependiendo del tamaño de su organización un plan de proyecto para la implementación de un Centro de Operaciones de Seguridad (SOC). El objetivo es establecer un servicio de ciberseguridad eficaz que permita detectar, analizar y responder a las amenazas y eventos de seguridad "en tiempo real".

Y esta es una de las primeras preguntas que hemos de resolver, ¿hemos de resolver en tiempo real estas amenazas? ¿ha de hacerse para todos los activos de la organización? ¿ha de utilizarse una única tecnología? ¿se ha de entrenar al equipo en todas las técnicas y tácticas de la matriz MITRE ATT &CK). Tratemos de dar algunas respuestas a lo largo de las siguientes secciones.

El plan se estructura en cuatro áreas clave: definición del alcance, selección de la ubicación, selección de tecnologías y selección de personal.

Estas directrices aseguran que el servicio esté alineado con los objetivos estratégicos de la organización, cumpla con los requisitos regulatorios y cuente con el personal y la tecnología adecuados para operar de forma eficiente y segura.

6.2. DEFINICIÓN DE ALCANCE

La definición del alcance es el primer paso crítico para garantizar que el SOC cumpla con los objetivos estratégicos y operativos de la organización. Para realizar una adecuada evaluación, este proceso debe incluir:

Asignación presupuestaria: No es casual el empezar la definición del alcance con la pregunta de cuánto nos va a costar ya que en la mayoría de los casos no podremos cubrir, bien en extensión, bien en profundidad todos aquellos recursos críticos a proteger. Tanto los recursos, o activos críticos, como la profundidad o casos de uso, serán estudiados en las siguientes secciones. En cuanto al ejercicio que cualquier CISO ha de hacer es establecer cuáles serán los costes de adopción y operación:

- **Adopción:** En este apartado no sólo nos hemos de enfocar en la selección adecuada de los modelos de despliegue de un SOC, que puede incluir (o no) la selección de herramientas y tecnología, sino aquellos desarrollos internos que sean requeridos para la generación de los logs necesarios, si estos no están disponibles previamente, su salvaguarda y los canales y procesos de entrega. Estos costes pueden verse minimizados en parte por la selección de SOCs de última generación que disponen de mecanismos ya preparados, pero hemos de considerar que estas capacidades vendrán a engrosar los costes de operación.

  Por otro lado y con independencia del alcance y del modelo siempre habrá que considerar los procesos de mejora continua, éstos son aquellos que nos obligarán a descartar casos de usos previsto, la creación de otros nuevos o la modificación de los existentes. Asimismo, la eventual expansión hacia áreas aún no monitorizadas han de ser consideradas en la confección del presupuesto de adopción. Por último, un factor relevante es el establecimiento de las ventanas de monitorización, es frecuente que un servicio SOC se ofrezca en 24x7, pero dependiendo del sector, la criticidad de los sistemas y la madurez y capacidad de la organización para dar respuesta pueda ser negociada a otros modelos menos agresivos.

- **Operación:** establecer los costes de operación incluso en aquellos casos en los que se haya seleccionado un MSSP para la gestión completa de un servicio de SOC. Además de los costes del personal propio, son relevantes aquellos que conllevan la gestión y respuesta ante incidentes, las eventuales importes adicionales del proveedor para la activación de equipos DFIR , licencias de los diferentes productos, incrementos debidos a la ingesta adicional de logs o crecimiento de las infraestructuras así como la capacitación no sólo del personal de seguridad sino de todas aquellas áreas que hayan de dar soporte a posibles incidentes.

Identificación de activos críticos: de acuerdo con las prioridades del negocio los sistemas, datos y procesos que requieren protección prioritaria han de ser identificados. Es indudable que cuando se plantea la conversación con la dirección de la organización, la respuesta a la pregunta de qué es crítico, sea… 'todo', sin embargo el despliegue de un SOC requiere un análisis detallado para encontrar el equilibrio entre eficacia y coste. Algunos criterios para la correcta selección del alcance serían:

- Seleccionar las aplicaciones con mayor 'peso' dentro de la organización, aunque existen varios criterios para seleccionarlas. Se han de considerar, aquellas que generen mayores beneficios.

- Un vector que también puede ayudarnos, puede ser el nivel de exposición a los atacantes.

- También todos los sistemas auxiliares de tecnología que ayudan a la operación desde el punto de vista interno, como, plataformas de gestión de redes y comunicaciones, soluciones de autenticación, soluciones para el mantenimiento de las actualizaciones, plataformas para la gestión de cuentas privilegiadas, sistemas de almacenamiento y backup..deberían de ser considerados dentro de estas primeras listas.

- Mención aparte requiere el entorno en el que nuestros activos se desplieguen. El tratamiento y selección variará si hablamos de entornos IT tradicionales, entornos Cloud, entornos móviles, entornos IoT, OT o lo que seguramente sea más común, entornos híbridos.

Selección de casos de uso: los casos de uso se definen como cada uno de los escenarios específicos que describe cómo el SOC debe de actuar, es decir, qué parámetros utilizará para detectarlo y analizarlo y así poder responder. De manera habitual, estos casos de uso se compondrán por uno o más escenarios que vendrán generados por indicadores de compromiso de uno o más sistemas de alerta que nos permitan realizar esta correlación. Enseguida, será evidente que el listado será extenso incluso con pocos casos de uso, lo cual nos obligará a una priorización de los mismos y la definición consciente de los activos a monitorizar. En el siguiente diagrama se plantea (a modo de ejemplo visual) una posible relación de los elementos que componen los casos de uso para un eventual objetivo estratégico denominado "Protección de datos personales para la aplicación APP101":

OBJETIVO ESTRATÉGICO

Protección de datos personales en APP101

Caso de uso 1
Actividad de red anómala

Caso de uso 2
Archivos modificados inesperadamente

Caso de uso 3
Actividad de usuario sospechosa

`Escenario 1`
Tráfico inusual hacia IPs externas

`Escenario 2`
Aumento de conexiones fallidas

`Escenario 3`
Cambios en archivos del sistema

`Escenario 4`
Creación de archivos sospechosos

`Escenario 5`
Intentos de acceso fuera de horario

`Escenario 6`
Múltiples intentos de inicio de sesión fallidos

1. Logs de firewall

2. Logs de IDS/IPS

3. Logs de tráfico de red

4. Logs de sistema

5. Logs de auditoría

6. Log XDR

7. Logs de auditoría de ususario

8. Logs de autenticación y acceso

En esta línea, y para completar el listado de los requisitos técnicos relacionados con los logs y fuentes de datos que crearían los escenarios y casos de uso para al objetivo estratégico “Protección de los datos personales en la aplicación ficticia APP101” serían:

1. Logs de firewall:
- Registro de tráfico entrante y saliente.
- Bloqueos y permisos de conexiones.

2. Logs de IDS/IPS:
- Detección de intrusiones.
- Alertas de posibles ataques.

3. Logs de tráfico de red:
- Análisis de patrones de tráfico.
- Identificación de anomalías.

4. Logs de sistema:
- Registro de eventos del sistema operativo.
- Cambios en archivos críticos.

5. Logs de integridad de archivos:
- Monitoreo de cambios en archivos.
- Alertas de modificaciones no autorizadas.

6. Logs de antivirus/XDR:
- Detección de malware.
- Escaneos y resultados de análisis.

7. Logs de autenticación:
- Intentos de inicio de sesión.
- Éxitos y fracasos de autenticación.
- Registro de accesos a recursos.
- Permisos y denegaciones.

8. Logs de auditoría de usuario:
- Actividades del usuario.
- Acciones realizadas y recursos accedidos.

Como conclusión, la definición del alcance es fundamental para asegurar que el SOC cumpla con los objetivos estratégicos y operativos de la organización. Este proceso incluye la asignación presupuestaria, la identificación de activos críticos y la selección de casos de uso, permitiendo una protección eficaz de los recursos críticos de la organización, optimizando costos y garantizando una respuesta efectiva ante incidentes.

Además, se recomienda establecer un documento de alcance formal que incluya los límites del servicio, casos de uso, posibles exclusiones, canales de comunicación entre el SOC y la empresa, procesos de monitorización del propio servicio, SLA esperados y mecanismos de revisión periódica (con independencia del modelo de SOC seleccionado).

6.3. SELECCIÓN DE LA **UBICACIÓN**

Para la ubicación del SOC o de los componentes del MSSP se debe considerar tanto aspectos técnicos como estratégicos.

Dependiendo del modelo de despliegue interno, híbrido o completamente gestionado por terceros, así como los activos que debemos monitorizar teniendo en cuenta su criticidad, se deberá optar por una ubicación física y lógica que garantice la segmentación de zonas (colección, análisis, notificación, administración, cobertura 24x7x365) y cumplir con requisitos de seguridad física y lógica.

Otro factor importante a tener en cuenta es el cumplimiento normativo. La ubicación debe respetar las leyes de soberanía de datos, especialmente si se manejan datos personales o sensibles.

También es importante tener en cuenta la soberanía digital. Proveedores y fabricantes de determinados países, como EEUU y China, están sujetos a normativas, que puede suponer una pérdida de confidencialidad de los datos, incluso aunque los datos se encuentren en la Unión Europea.

Asi mismo, debe coordinarse con los planes de redundancia y continuidad, y se deben considerar sitios alternativos o capacidades de recuperación ante desastres (DRP/BCP).

Por otro lado, la ubicación seleccionada debe asegurar conectividad segura con los sistemas del cliente mediante VPNs, enlaces dedicados o gateways cifrados.

CREST recomienda que la ubicación esté respaldada por controles de acceso físico, monitoreo ambiental y segregación de funciones.

A modo resumen, todas las ubicaciones tienen sus ventajas y desventajas:

Ubicación	Ventajas	Desventajas
En las instalaciones corporativas	• Control total • Fácil integración con IT	• Coste alto • Limitada escalabilidad
En centro de datos seguro	• Infraestructura robusta • Alta disponibilidad	• Menos control físico • Dependencia externa
Cloud SOC (SOC como servicio - MSSP)	• Escalabilidad • Bajo costo inicial	• Dependencia de terceros • Posible pérdida de control
Ubicaciones geográficamente diversificadas	• Cobertura global • Resiliencia	• Complejidad de gestión • Diferencias legales

Cómo conclusión: la ubicación de un SOC puede ser interna, externa o una combinación de ambas (híbrida). La decisión depende de factores como la disponibilidad de talento, la infraestructura tecnológica, la proximidad a otras instalaciones críticas y las consideraciones de seguridad física entre otros.

6.4. SELECCIÓN DE **PERSONAL**

El éxito de un SOC depende en gran medida del talento humano. Se trata de un servicio proporcionado por un grupo de profesionales que coordinados y junto a las herramientas correctas son capaces de monitorizar y proteger 24 x 7 los activos de la organización. Gracias a ellos se puede hablar de SOC, y actualmente son un factor fundamental para el correcto funcionamiento del SOC.

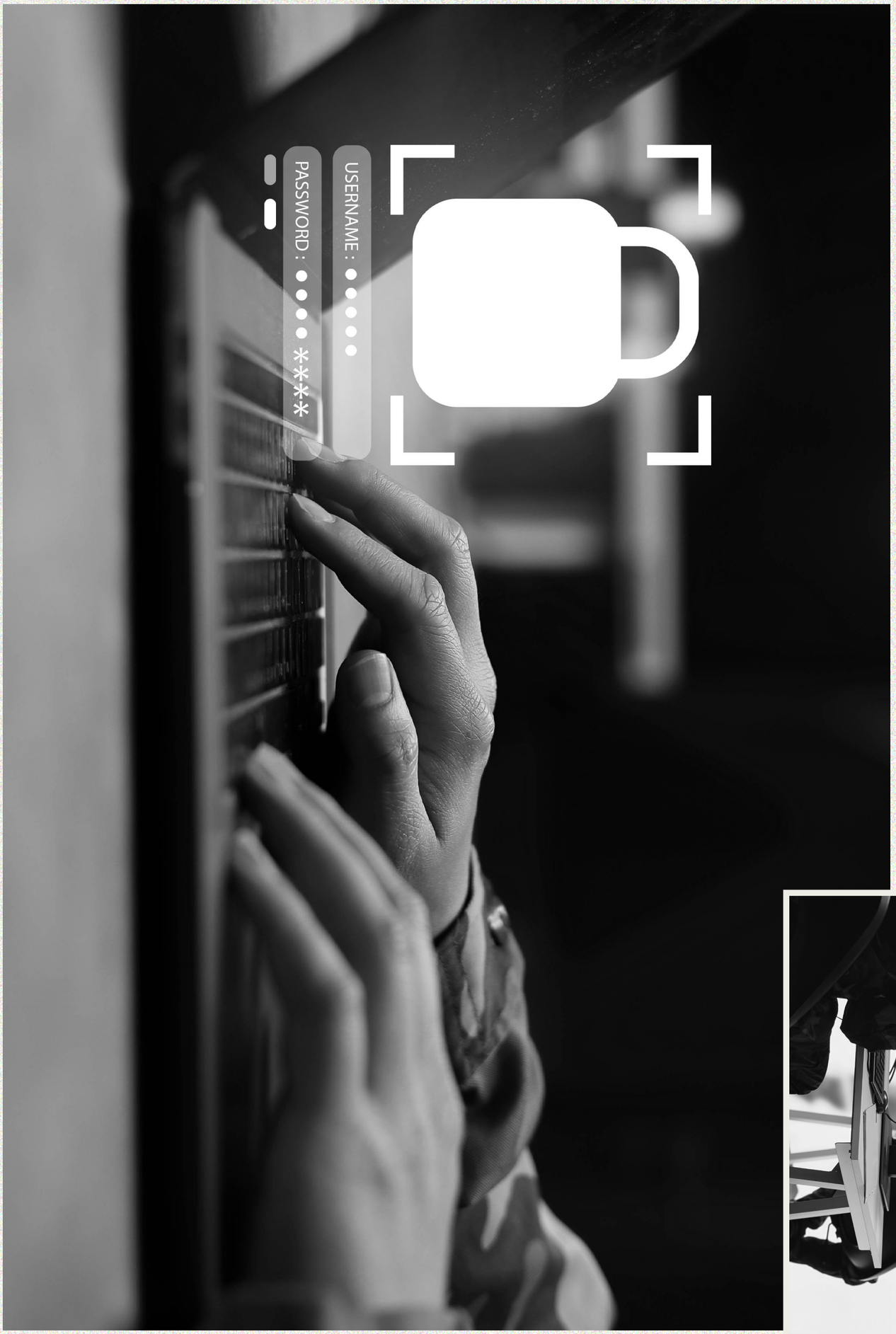
Hay que tener en cuenta que, por regla general, el personal necesario se organiza por niveles de actuación, y la experiencia, capacidad y especialización que se requiere para cada nivel aumenta proporcionalmente según la complejidad ascendente de los propios niveles.

Por otro lado, a la hora de seleccionar el personal, hay que tener en cuenta que cada modelo de SOC es diferente, y cómo vimos en el punto anterior no es lo mismo la operativa de un SOC interno, Servicios gestionados de seguridad (MSSP / MDR) u SOC OT. Por ejemplo, en el caso de los SOC de MSSP / MDR es necesario una figura responsable de comunicación por ambas partes ya que se está externalizando esta capacidad. Otro ejemplo es que las personas a contratar son diferentes en función de las tecnologías que deben monitorizar o analizar, siendo casos muy diferente entornos OT a los de IT interno o servicios cloud.

Por lo general a la hora de evaluar capacidades de personal, las certificaciones recomendadas pueden ser las siguientes: CISSP, CISM, CEH, GCIA, GCIH, OSCP, BTL1, OSEP, OSWP, MAD20, eJPT, CRTO, entre otras. También es muy positivo la formación continua y simulacros: ejercicios de Red Team/Purple Team, tabletop exercises y participación en comunidades (FIRST, CSIRT.es, etc.).

La conclusión es que la selección de personal para un SOC es fundamental. Se debe buscar profesionales con habilidades en ciberseguridad, análisis de amenazas, respuesta a incidentes y gestión de vulnerabilidades. Además, es importante fomentar un ambiente de trabajo colaborativo y continuo desarrollo profesional.

7. TECNOLOGÍAS USADAS EN UN SOC



Un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) depende en gran medida de una arquitectura tecnológica avanzada para cumplir su misión: detectar, analizar, responder y prevenir amenazas de ciberseguridad tanto en los entornos corporativos (IT) como en entornos Operacionales (OT), tal y como hemos comentado en anteriores capítulos. Estas tecnologías no son estáticas ni universales, sino que evolucionan rápidamente en función del contexto organizacional, el perfil de amenazas, la madurez del SOC y las tendencias del mercado.

En este capítulo, se describe un panorama estructurado de las tecnologías más relevantes que conforman un SOC moderno, con base en los marcos de referencia, estudios analíticos del sector y las mejores prácticas identificadas por organismos especializados.

7.1. SELECCIÓN DE **TECNOLOGÍAS**

Sistemas SIEM
(Security Information and Event Management)

El SIEM es el sistema central de recogida, correlación y análisis de eventos de seguridad y operacionales. Esta tecnología permite centralizar la visibilidad sobre los activos organizativos, identificar patrones de comportamiento anómalos y generar alertas contextualizadas.

Los sistemas SIEM modernos han evolucionado más allá del análisis de logs tradicional, incorporando capacidades como:

- Correlación basada en Inteligencia Artificial (IA) y Machine Learning (ML).
- Enriquecimiento de eventos con datos de contexto (geolocalización, usuario, criticidad del activo, dependencias de otros activos, etc).
- Capacidades de visualización avanzada y paneles personalizables.
- Integración con herramientas de automatización y fuentes de inteligencia de amenazas (Feeds).

Según diversos informes de mercado como, Cuadrante Mágico de Gartner[1] para SIEM o el Forrester Wave[2], se observa una tendencia clara hacia modelos de SIEM cloud-native, flexibles, y orientados a ofrecer una experiencia más proactiva al analista y con capacidades de automatización gracias a la IA.

[1]https://www.gartner.com/reviews/market/security-information-event-management
[2]https://www.forrester.com/blogs/announcing-the-forrester-wave-security-analytics-platforms-2025-the-siem-vs-xdr-fight-intensifies/

Plataformas SOAR
(Security Orchestration, Automation and Response)

El SOAR complementa al SIEM permitiendo automatizar respuestas a incidentes y orquestar tareas complejas entre distintos sistemas del ecosistema de seguridad. El valor del SOAR radica en reducir el tiempo medio de respuesta (MTTR) y aumentar la consistencia de la respuesta mediante playbooks.

- Funcionalidades comunes incluyen:

Automatización de tareas repetitivas (ej. bloqueos, envíos de notificación, aislamiento de activos, exclusiones, etc).

- Gestión de casos e investigaciones.
- Recolección de evidencias y trazabilidad para cumplimiento normativo.

Según estudios recientes del sector destacan la consolidación de SOAR dentro de suites integradas de seguridad, así como su papel clave en la reducción de la fatiga del analista y la carga operativa.

EDR y XDR
(Endpoint / Extended Detection and Response)

El SOAR complementa al SIEM permitiendo automatizar respuestas a incidentes y orquestar tareas complejas entre distintos sistemas del ecosistema de seguridad. El valor del SOAR radica en reducir el tiempo medio de respuesta (MTTR) y aumentar la consistencia de la respuesta mediante playbooks.

- Funcionalidades comunes incluyen:

Automatización de tareas repetitivas (ej. bloqueos, envíos de notificación, aislamiento de activos, exclusiones, etc).

- Gestión de casos e investigaciones.
- Recolección de evidencias y trazabilidad para cumplimiento normativo.

Según estudios recientes del sector destacan la consolidación de SOAR dentro de suites integradas de seguridad, así como su papel clave en la reducción de la fatiga del analista y la carga operativa.

[1]https://www.gartner.com/reviews/market/security-information-event-management
[2]https://www.forrester.com/blogs/announcing-the-forrester-wave-security-analytics-platforms-2025-the-siem-vs-xdr-fight-intensifies/

NDR
(Network Detection and Response)

Las soluciones NDR ofrecen capacidades de detección basadas en inspección del tráfico de red, lo que permite identificar amenazas incluso en dispositivos sin agente o en entornos segmentados (como OT/IoT/IIoT/IoMT).

Incluyen funcionalidades como:

- Análisis de tráfico de Red en tiempo real.
- Detección de patrones de exfiltración, movimiento lateral o uso indebido de protocolos.
- Identificación de anomalías basadas en comportamiento y patrones históricos.

En entornos híbridos y críticos, el NDR proporciona una capa adicional de visibilidad que complementa otras tecnologías como EDR o SIEM. Según estudios de mercado, es una pieza cada vez más demandada en SOCs maduros.

Plataformas de Inteligencia de Amenazas
(Threat Intelligence Platforms - TIP)

La inteligencia de amenazas proporciona el contexto necesario para convertir datos en conocimiento accionable. Las plataformas TIP permiten gestionar de forma estructurada los indicadores de compromiso (IoCs), las campañas de amenazas, los actores maliciosos y los patrones de TTPs (técnicas, tácticas y procedimientos).

Funciones habituales:

- Agregación y correlación de múltiples fuentes de inteligencia.
- Clasificación y priorización de amenazas según su relevancia.
- Integración con herramientas de detección (SIEM, SOAR) para enriquecer alertas.

Modelos de referencia como MITRE ATT&CK[1] se integran habitualmente con estas plataformas de inteligencia para estructurar la información de forma táctica.

Gestión de vulnerabilidades

El SOC debe contar con una visibilidad clara de las debilidades de los sistemas que protege. La gestión de vulnerabilidades permite:

- Identificar exposiciones conocidas en sistemas, aplicaciones y servicios.
- Priorizar la remediación en función del riesgo, la criticidad del activo y la explotabilidad.
- Integrar los hallazgos con el análisis de amenazas para una respuesta más efectiva.

Los marcos de gestión de riesgo como CVSS (Common Vulnerability Scoring System) y las metodologías basadas en riesgo son ampliamente usados para la priorización

[1] https://attack.mitre.org/

[2] https://www.forrester.com/blogs/announcing-the-forrester-wave-security-analytics-platforms-2025-the-siem-vs-xdr-fight-intensifies/

UEBA (User and Entity Behavior Analytics)

UEBA aporta una capa analítica basada en el comportamiento de usuarios y entidades, detectando desviaciones frente a patrones normales. Es especialmente útil para identificar amenazas internas, compromisos de cuentas o accesos indebidos.

Capacidades clave:

- Modelado del comportamiento habitual de usuarios y dispositivos.
- Detección de actividades anómalas o no autorizadas.
- Asignación de niveles de riesgo por usuario o sistema.

Su integración con SIEM o XDR permite detectar amenazas sin depender de reglas predefinidas.

Monitorización de entornos cloud y modernos

La transformación digital ha llevado al SOC a extender su alcance hacia entornos cloud y de aplicaciones nativas en la nube. Para ello se integran tecnologías como:

- CSPM (Cloud Security Posture Management): análisis y remediación de configuraciones inseguras.
- CWPP (Cloud Workload Protection Platforms): protección de cargas de trabajo virtualizadas y contenedores.
- CNAPP (Cloud-Native Application Protection Platform): plataformas que unifican visibilidad y protección desde la fase de desarrollo hasta la operación.

El estudio "Market Guide for Cloud-Native Application Protection Platforms" de Gartner señala una convergencia clara de estas soluciones como respuesta a la creciente complejidad cloud.

Herramientas auxiliares:
ticketing, gestión, colaboración

Además de las herramientas puramente de seguridad, un SOC requiere tecnologías que faciliten su operación:

- Sistemas de ticketing e ITSM para gestionar flujos de trabajo.
- Herramientas colaborativas para coordinación entre equipos.
- Plataformas de documentación y lecciones aprendidas.
- Dashboards de gestión para supervisión operativa y estratégica.

La alineación de estas herramientas con los procesos del SOC es clave para su eficacia y trazabilidad.

[1] https://www.gartner.com/reviews/market/security-information-event-management

[2] https://www.forrester.com/blogs/announcing-the-forrester-wave-security-analytics-platforms-2025-the-siem-vs-xdr-fight-intensifies/

7.2. HERRAMIENTAS

Open Source

Tabla de Herramientas Open Source (equivalentes por categoría):

Dominio	Soluciones habituales
SIEM	ELK Stack + Wazuh / OpenSearch Dashboards / Graylog
SOAR	TheHive + Cortex / Shuffle / DFIR IRIS
EDR / XDR	Wazuh (modo EDR) / Velociraptor / Osquery / KataOS telemetry
NDR	Zeek / Suricata / Arkime (full-packet capture)
TIP	MISP / OpenCTI
Gestión de vulnerabilidades	OpenVAS/Greenbone CE / Nmap+Vulners / OWASP Dependency-Check
UEBA	ELK ML jobs / Apache Spot / SnowcatCloud UEBA
Cloud / CNAPP	Falco / Kube-Bench / Trivy / Open Policy Agent (OPA)
Herramientas auxiliares	GLPI / OTRS / Zammad / Mattermost / Wiki.js

Ventajas OSS: coste de licencia nulo, capacidad de personalización, comunidad activa.
Retos: curva de aprendizaje, mantenimiento, cobertura limitada en OT nativo.

Herramientas Propietarias (IT/OT)

Tabla de Herramientas propietarias (IT y OT):

Dominio	Soluciones comerciales más implantadas (según Cuadrantes de Gartner / Forrester Wave 2024-25)
SIEM (IT)	Splunk / IBM QRadar / Microsoft Sentinel / Securonix / Exabeam
SOAR	Palo Alto Cortex XSOAR / IBM Resilient / Swimlane / Tines
EDR / XDR	CrowdStrike Falcon / SentinelOne / Microsoft Defender / Palo Alto Cortex XDR / Trend Micro Vision One
NDR	Vectra AI / Darktrace / ExtraHop / Cisco Secure Analytics / Corelight (Sensor)
TIP	Recorded Future / Anomali / ThreatConnect / Mandiant Advantage Intel
Gestión de vulnerabilidades	Tenable .sc / Nessus / Qualys VMDR / Rapid7 InsightVM
UEBA	Exabeam / Securonix / LogRhythm UEBA / Gurucul
CNAPP / Cloud	Wiz / Prisma Cloud / Orca Security / Microsoft Defender for Cloud
ITSM / Ticketing	ServiceNow / Jira Service Management / BMC Helix
OT Visibility & Detection	Dragos / Nozomi Networks / Claroty / Tenable.ot / Cisco Cyber Vision
OT Asset Management	Forescout / Radiflow / Hexagon PAS

Tendencias:
- Convergencia SIEM + XDR + SOAR en plataformas unificadas.
- Integración nativa IT/OT para visibilidad industrial.
- Uso de IA generativa para acelerar investigación y playbooks.

7.3. CONCLUSIONES

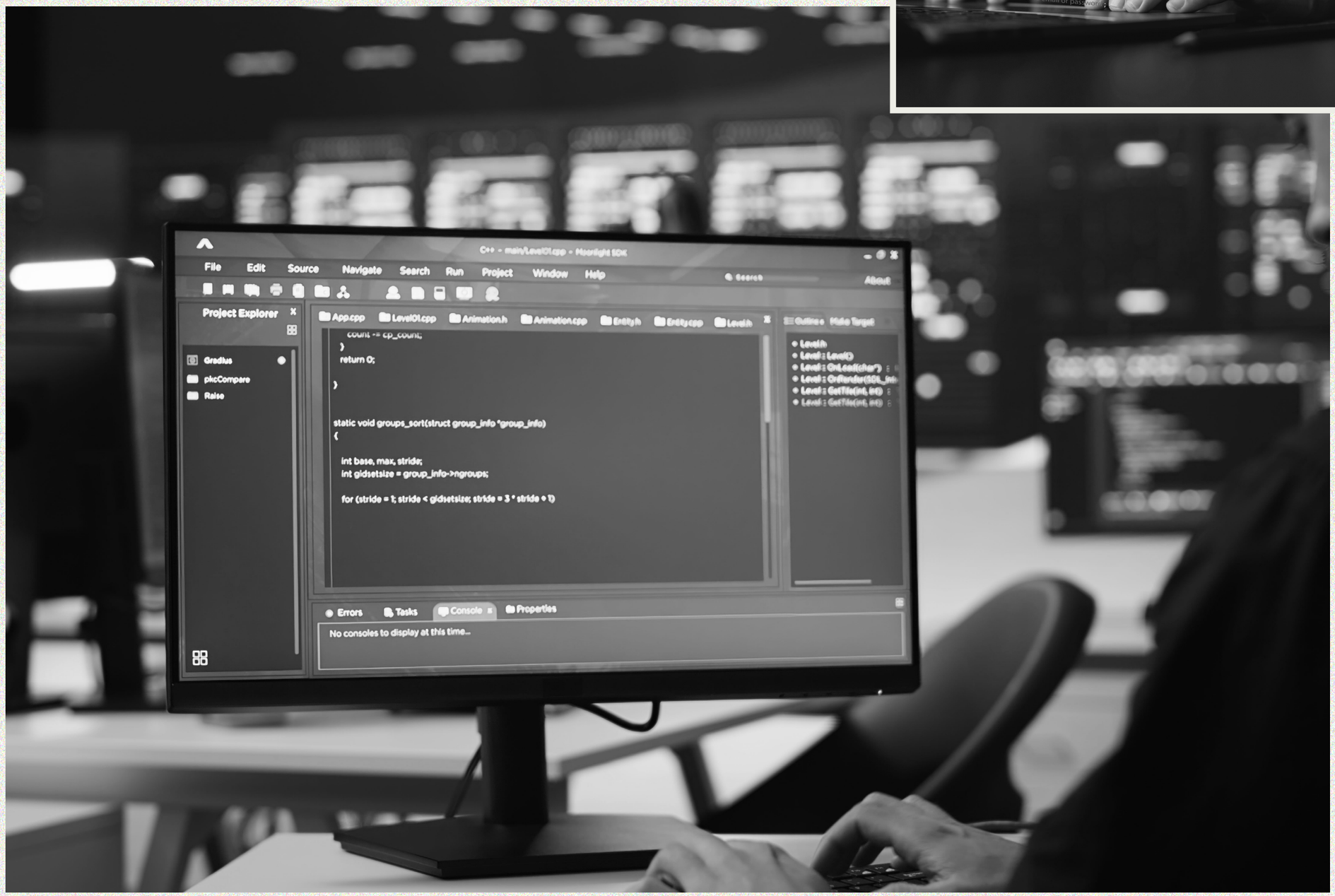
El ecosistema tecnológico de un SOC debe ser flexible, interoperable y orientado a la acción. No se trata únicamente de contar con la tecnología más avanzada, sino de integrarla de forma coherente con los procesos, las personas y los objetivos del negocio. Los estudios más recientes en el ámbito de la ciberseguridad insisten en la necesidad de entornos centrados en la automatización, la inteligencia contextual y la visibilidad unificada, como pilares para afrontar con éxito los desafíos actuales y futuros en la protección de los activos digitales.

Aunque la elección de soluciones específicas debe alinearse con las necesidades y madurez de cada organización, son necesarios informes que permitan establecer comparativas objetivas y seguir la evolución de las capacidades clave. En particular, Gartner ha resaltado en sus guías más recientes la tendencia a la convergencia de soluciones en plataformas unificadas (como CNAPP), la automatización basada en contexto y la necesidad de una visibilidad multidominio (endpoint, red, identidad y nube) para hacer frente a las amenazas actuales.

En definitiva, la tecnología en un SOC no es un fin en sí misma, sino un habilitador para una defensa eficaz, eficiente y alineada con la estrategia de ciberseguridad de la organización.

CERTIFICACIONES Y GRUPOS DE INTERÉS

8.



Aunque se trate de una afirmación repetida, no deja de ser cierta: las organizaciones enfrentan hoy un volumen cada vez mayor de incidentes de seguridad, con una complejidad y un alcance en constante crecimiento.

Según el informe M-Trends 2025 de Mandiant[1], el dwell time (número de días que un atacante permanece en un entorno comprometido antes de ser detectado), ha pasado de los 205 días de 2014 a los 11 días de 2024.

En el ecosistema de los Centros de Operaciones de Seguridad (SOC) y los equipos de respuesta a incidentes (CERT/CSIRT), tanto las certificaciones profesionales como la pertenencia a grupos de colaboración especializados desempeñan un papel fundamental, aunque con enfoques distintos.

Las certificaciones contribuyen directamente a mejorar la calidad del servicio, fortaleciendo las capacidades técnicas y procedimentales de los equipos, lo que se traduce en una detección más temprana de incidentes. Por otro lado, la colaboración y adhesión a grupos de interés o redes colaborativas, permite la posibilidad de compartir información clave sobre nuevas amenazas, tácticas adversarias, vulnerabilidades emergentes o tecnologías defensivas, lo que facilita mejoras en la capacidad de detección y puede contribuir significativamente a la reducción del dwell time.

Certificaciones y membresías a grupos de interés, permiten validar la madurez del equipo, mejorar continuamente sus capacidades y formar parte de una comunidad global que comparte el objetivo común de proteger el ciberespacio.

Este capítulo presenta las principales certificaciones reconocidas en el ámbito de la ciberseguridad, así como los grupos de colaboración más relevantes, destacando su valor estratégico para los equipos de respuesta.

En este escenario, la ciberseguridad ya no puede abordarse únicamente como un asunto operativo, sino como un elemento central en la agenda estratégica de la organización. La complejidad de las amenazas, sumada a la creciente dependencia de infraestructuras digitales y servicios críticos, obliga a las compañías a adoptar un enfoque proactivo, con capacidades de monitorización, detección y respuesta en tiempo real.

Disponer de un centro de operaciones de seguridad (SOC) deja de ser una opción para convertirse en un pilar estratégico, que no solo protege los activos más valiosos, sino que también respalda la continuidad del negocio y la confianza de clientes, socios y reguladores.

Sobre cómo llevar a la práctica este modelo y cuáles son los factores clave de éxito en su implementación, resulta fundamental conocer la visión de los expertos en ciberseguridad, quienes aportan un conocimiento profundo del terreno y una experiencia decisiva en la construcción de estas capacidades.

[1] https://cloud.google.com/security/resources/m-trends?hl=es-419

8.1. CERTIFICACIONES **RELEVANTES**

Una de las decisiones estratégicas más relevantes es la selección de certificaciones de seguridad que alineen la operación del SOC con los objetivos de la organización, los requisitos regulatorios y las expectativas de los clientes.

Para ello, debemos tener en cuenta factores como el tipo de organización, los clientes y mercados objetivo o el nivel de madurez.

Según esto, en el caso del SOC de una organización privada cuyo objetivo sea el a su vez dar servicios a otras organizaciones que no sean del ámbito público, se podría considerar la certificación ISO27001:2022. Con este mismo objetivo, pero para el caso de organizaciones cuyo mercado objetivo se encuentra en USA y LATAM, sería una opción muy interesante la certificación SOC2.

Por otro lado, tanto si la organización es un organismo público español como si es una organización privada con el objetivo de dar servicio a entidades públicas, será obligatorio el alcanzar la certificación ENS. No obstante, como paso adicional y diferenciador respecto al mero cumplimiento del ENS, se recomienda la adopción del Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados (PCE-SSG), recogido en la Guía CCN-STIC 896, que establece requisitos específicos para la prestación de servicios de seguridad gestionados, reforzando la alineación con el Esquema Nacional de Seguridad y aportando un nivel superior de madurez y robustez.

Las certificaciones CREST (Council of Registered Ethical Security Testers) son acreditaciones internacionales en el ámbito de la ciberseguridad que buscan establecer estándares de calidad, ética y competencia técnica en servicios de seguridad. CREST es una organización sin fines de lucro reconocida a nivel mundial.

Cuando el nivel de madurez es superior y se quiere poner énfasis en la resiliencia y continuidad de negocio se puede optar por la certificación ISO22301.

Como vemos, no existe una única certificación ideal. La clave está en alinear la estrategia de certificación con los objetivos del SOC y las necesidades del negocio. En muchos casos, una combinación de certificaciones proporciona una cobertura más robusta y diferenciadora.

Certificación	Descripción	Valor dentro del SOC
ISO/IEC 27001	Estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Su adopción por parte de un SOC o CSIRT garantiza que la organización: - Gestiona los riesgos de seguridad de forma sistemática. - Aplica controles técnicos y organizativos adecuados. - Cumple con requisitos legales y contractuales. - Mejora continuamente sus procesos de seguridad.	Aporta una base sólida de gobernanza y control, facilitando la confianza de clientes y socios, y alineando las operaciones con buenas prácticas internacionales. Es frecuentemente requerido por entidades privadas en el entorno europeo. Reconocida internacionalmente, ideal para organizaciones con presencia global
Esquema Nacional de Seguridad (ENS)	Marco normativo español que establece los principios y requisitos mínimos para la protección de la información en el sector público y entidades que colaboran con él. Clasifica los sistemas en niveles (básico, medio, alto) y define medidas de seguridad asociadas.	Es esencial para operar en entornos públicos en España, asegurando la interoperabilidad, la trazabilidad y la protección de los servicios críticos. Es obligatoria para entidades públicas (AAPP) y para proveedores que deseen trabajar con la administración en España.
SOC 2 (System and Organization Controls)	SOC 2 es un estándar desarrollado por el AICPA (American Institute of Certified Public Accountants) que evalúa los controles internos de una organización en relación con cinco principios: seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad.	Refuerza la confianza de clientes internacionales, especialmente en entornos cloud y servicios gestionados, al demostrar el cumplimiento de controles rigurosos en la operación del SOC. Es muy reconocida por entidades privadas en Estados Unidos y, por extensión, en LATAM.
ISO/IEC 22301	La norma ISO/IEC 22301 es un estándar internacional para la gestión de la continuidad del negocio. Establece un marco para identificar amenazas potenciales, evaluar su impacto y desarrollar planes de respuesta que aseguren la continuidad de los servicios críticos ante interrupciones	Refuerza la resiliencia operativa del equipo, asegurando que los servicios de respuesta a incidentes puedan mantenerse activos incluso en situaciones de crisis o desastres. Facilita la planificación de contingencias y la recuperación rápida ante eventos disruptivos. Es requerido por entidades privadas en el entorno europeo, especialmente aquellas organizaciones con alta dependencia de la disponibilidad del servicio
CREST	Garantizan que la compañía cumple con procesos, políticas, metodologías y controles de calidad en áreas como: - Penetration Testing (pruebas de intrusión). - Red Teaming (simulación de ataques avanzados). - Incident Response (respuesta ante incidentes). - Threat Intelligence (inteligencia de amenazas)	CREST es una garantía de que la empresa no solo tiene personal técnico competente, sino que también opera con procesos controlados y auditados, lo que aumenta su reputación y competitividad internacional
CCN-STIC 896 (PCE-SSG)	Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados, que define requisitos adicionales sobre ENS para SOC que prestan servicios gestionados.	Aporta un nivel superior de madurez y diferenciación, reforzando la confianza en la prestación de servicios críticos y alineando la operación con estándares nacionales avanzados.

8.2. GRUPOS DE INTERÉS Y **COLABORACIÓN**

Uno de los pilares fundamentales para fortalecer la defensa frente a las ciberamenazas actuales es la colaboración activa y el intercambio de información entre entidades. En un entorno donde los ataques son cada vez más sofisticados, automatizados y persistentes, ninguna organización puede defenderse de forma aislada. La inteligencia colectiva se ha convertido en un recurso estratégico clave.

Esta colaboración, se articula a través de diferentes foros de referencia según alcance geográfico. La participación en este tipo de foros no sólo sirve para mejorar la capacidad de defensa a través de la inteligencia colectiva, también requiere alinear la operativa con estándares internacionales, fomenta la madurez del SOC al exponerlo a escenarios reales y, finalmente, refuerza la confianza entre organizaciones, creando un ecosistema global más seguro.

De esta forma, se fomenta la detección temprana de amenazas al compartir indicadores de compromiso (IoCs), tácticas, técnicas y procedimientos (TTPs) que permiten a los SOC anticiparse a ataques que otros ya han sufrido, reduciendo el tiempo de detección y respuesta.

Al conocer cómo otras organizaciones han mitigado incidentes similares, se pueden aplicar medidas preventivas o correctivas más eficaces y rápidas, reduciendo significativamente el impacto.

Independientemente de la ubicación o sector, el intercambio de información permite tener una visión más completa y contextualizada del entorno de riesgo, dando una visibilidad global del panorama de amenazas.

Es por esto que compartir información no es una opción, sino una necesidad estratégica. La pertenencia activa a foros de referencia y redes de intercambio es una de las mejores inversiones que puede hacer un SOC para evolucionar de un enfoque reactivo a uno verdaderamente proactivo y colaborativo

FIRST

(Forum of Incident Response and Security Teams)

FIRST (https://www.first.org/) es una comunidad global de equipos de respuesta a incidentes creada en el año 1990 (apenas dos años después del famoso Gusano de Morris), con una clara intención de mejorar la cooperación entre los equipos de respuesta a incidentes de todo el mundo, promoviendo el intercambio de información, herramientas y mejores prácticas para enfrentar amenazas de seguridad informática, tal y como se indica en la definición de su misión.

Uno de los valores primordiales de FIRST además de la potenciar y promover la colaboración internacional, es la definición de diversos estándares de seguridad como:

- CVSS (Common vulnerability scoring system): Estandar de calificación de impacto y riesgo para las vulnerabilidades identificadas.
- EPSS (Exploit prediction scoring system): Estándar utilizado para la gestión y priorización de la corrección de vulnerabilidades.
- TLP (transfer light protocol): Estándar de clasificación de información utilizado a nivel internacional en la comunidad en la compartición y divulgación de información de ciberseguridad.
- CSIRT Services framework y PSIRT services framework, a los cuales se hace referencia en el capítulo 3 de este documento.

Foro referente a nivel internacional, ser miembro de FIRST es un sello de calidad y madurez operativa. El proceso de adhesión al foro FIRST está diseñado para asegurar que los equipos miembros cumplan con estándares de calidad y colaboración.

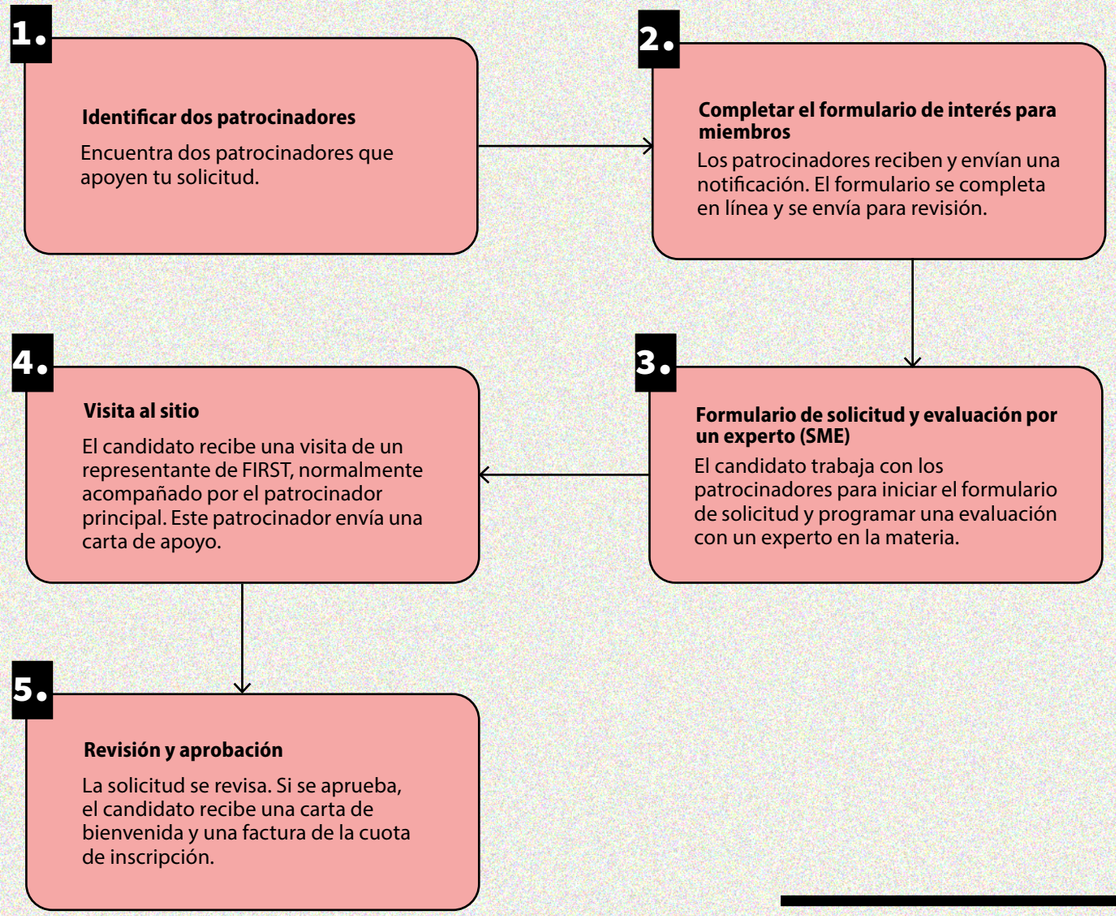
Actualmente existen tres tipos de miembros:

`Miembros plenos (Full Members):` Equipos de respuesta a incidentes que prestan servicios a una comunidad definida.

`Miembros asociados (Liaison Members):` Organizaciones o individuos con interés legítimo en la misión de FIRST, pero que no son equipos de respuesta.

`Miembros afiliados (Associates):` Entidades no lucrativas o académicas con valor añadido para la comunidad.

Cada uno de los tipos de miembros disponen de un proceso de adhesión diferente (https://www.first.org/membership/) siendo el más completo y más largo por su implicación, el relacionado con los miembros plenos o Full Members, cuyos pasos principales son los siguientes:



Se han de tener en cuenta las siguientes particularidades:

- El proceso completo puede durar aproximadamente 7 meses, aunque puede variar según la preparación del equipo y la disponibilidad de los patrocinadores.
- La membresía en FIRST implica un compromiso activo con la comunidad, incluyendo la participación en eventos, el intercambio de información y la colaboración en incidentes globales.

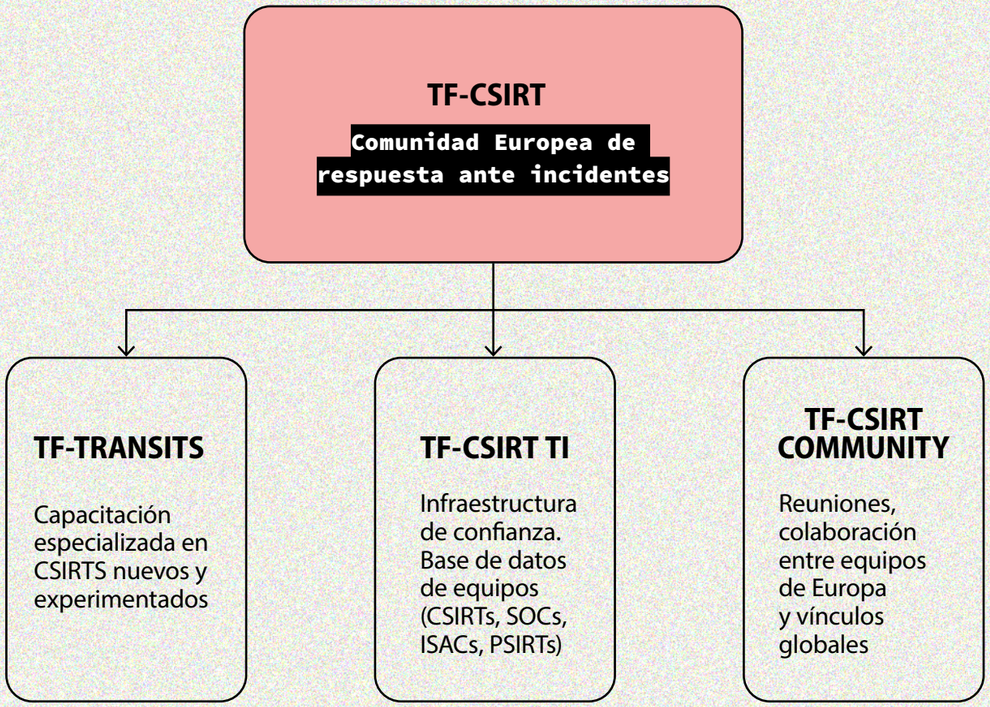
Este proceso garantiza que los equipos miembros de FIRST mantengan un alto nivel de profesionalidad, madurez operativa y capacidad de colaboración internacional.

TF-CSIRT

(Task Force - CSIRT)

TF-CSIRT (https://tf-csirt.org/) es una iniciativa europea creada en 1998, que agrupa a equipos de respuesta a incidentes, promoviendo la cooperación regional. Gestiona el servicio de acreditación Trusted Introducer (TI), que valida la existencia y calidad de los CSIRT.

Fuertemente vinculado a FIRST tanto en sus definiciones como es diversas colaboraciones y y eventos, a su vez proporciona una serie de funciones de forma particular las cuales se organizan en los que denominan tres Task Force:



TF-CSIRT utiliza el servicio Trusted Introducer (TI) como mecanismo de validación y gestión de su comunidad de equipos de respuesta a incidentes. El proceso de incorporación se estructura en varios niveles de madurez:

Nivel TI	Requisitos principales	Beneficios clave
TI Listed	• Es el primer paso para cualquier equipo que desee unirse. • Requiere proporcionar información básica del equipo y contar con el respaldo de la comunidad.	Permite visibilidad en el directorio TI y acceso limitado a servicios
TI Accredited	• Requiere haber estado previamente listado. • El equipo debe comprometerse a seguir buenas prácticas y aceptar las políticas establecidas por TI. • Implica una revisión más detallada de las capacidades y procesos del equipo	• Mayor credibilidad • Acceso ampliado a servicios y cooperación
TI Certified	• Requiere haber sido previamente acreditado. • El equipo debe demostrar un nivel de madurez operativo mediante una auditoría basada en el modelo SIM3 (Security Incident Management Maturity Model). • La auditoría es realizada por evaluadores autorizados de la comunidad TF-CSIRT.	• Máximo nivel de reconocimiento • Prueba de madurez operativa

A nivel general, la membresía supone un compromiso a largo plazo, ya que se espera que los equipos mantengan su estatus mediante mejoras continuas y revisiones periódicas.

RNS

(Red Nacional de SOCs)

La Red Nacional de SOC (RNS) (https://rns.ccn-cert.cni.es/) surge en 2021 como una iniciativa del CCN-CERT para interconectar los SOC de todo el territorio nacional, tanto públicos como privados, con el fin de detectar y bloquear de forma casi inmediata cualquier actividad sospechosa. Esta necesidad nació de la experiencia acumulada en la colaboración con distintos SOC y se vio reforzada por la Estrategia de Ciberseguridad de la Comisión Europea, que tras una oleada de ciberataques, apostó por una red europea de SOC apoyada en inteligencia artificial. La RNS busca así fortalecer la ciberdefensa nacional mediante una respuesta coordinada y ágil ante amenazas.

A diferencia de otros foros, lleva al extremo la filosofía de fomentar la compartición entre los SOCs de información sobre las tácticas, técnicas y procedimientos de nuevas amenazas, con el objetivo final de mejorar las capacidades de protección ante posibles ciberincidentes. Para ello, en base a su participación, establece los siguientes niveles a las entidades adheridas:

ORO	⟶	Nivel asignado a las entidades privadas y proveedoras con un nivel alto de participación
PLATA	⟶	Nivel asignado a las entidades privadas y proveedoras con un nivel de participación normal
INHABILITADO	⟶	Nivel asignado a las entidades privadas y proveedoras que han dejado de participar en la compartición de información.

La participación se mide a través de la información técnica compartida (a través de la plataforma MISP), que será valorada y puntuada en función de la naturaleza de la misma y su relevancia.

Dado que se pretende utilizar la RNS como una herramienta que mejore la seguridad de la información de las Administraciones Públicas, desde estas mismas Administraciones se podrá impulsar progresivamente la adopción de esta categorización de "Oro" y "Plata" como valores diferenciadores a la hora de evaluar propuestas comerciales de proveedores que opten a contratos públicos.

Para formar parte de la RNS, las entidades deben cumplir ciertos requisitos según su naturaleza: Las entidades públicas deben pertenecer al sector público español, registrar incidentes relevantes en LUCIA y contar con un SOC propio o en desarrollo; Las entidades proveedoras, aunque no sean públicas, deben ofrecer servicios de SOC a terceros y proteger activos españoles con su propio SOC; Por último, las entidades privadas que no prestan servicios a otras deben también disponer de un SOC que proteja activos en España.

Para aquellas entidades que cumplan lo anterior, el proceso de adhesión incluye:

1. Aceptación del código ético y de conducta profesional, obligatorio para todos los miembros.
2. Solicitud formal a través del formulario disponible en la plataforma oficial del CCN.
3. Certificación como SOC (cuando se publique la norma).
4. Utilizar las herramientas puestas a disposición por parte de la RNS tanto para estar al corriente de las comunicaciones como para intercambiar información técnica.

CSIRT.es

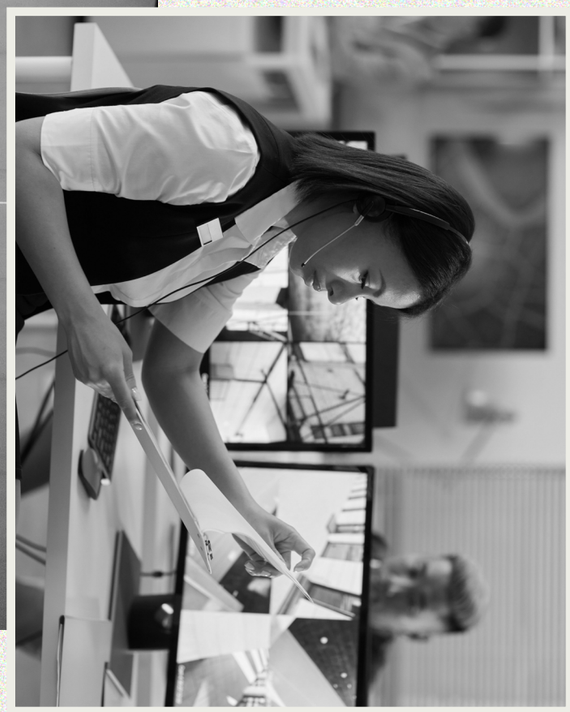
El Foro CSIRT.es (https://www.csirt.es/index.php/es/) es una plataforma independiente y sin ánimo de lucro que desde 2007 agrupa a los equipos de respuesta a incidentes de seguridad informática (CSIRTs) que operan en España. Su objetivo es fomentar la colaboración y coordinación entre estos equipos para mejorar la ciberseguridad en las redes nacionales. Los miembros deben ofrecer servicios relacionados con la gestión de incidentes. Como en los casos anteriores, el Foro promueve el intercambio de información útil y la visibilidad de sus miembros tanto a nivel nacional como internacional.

Ser miembro del Foro CSIRT.es aporta un gran valor a las entidades al integrarlas en una red de colaboración activa entre equipos de respuesta a incidentes de seguridad en España. Esta pertenencia permite compartir información crítica y de inteligencia sobre amenazas, coordinar acciones conjuntas ante incidentes relevantes y participar en proyectos que fortalecen la ciberseguridad nacional. Además, el Foro ofrece apoyo en la creación de nuevos CSIRTs y fomenta la cooperación con iniciativas similares a nivel nacional e internacional, lo que amplía la visibilidad y capacidades de cada entidad miembro.

El proceso de adhesión al Foro CSIRT.es está diseñado para garantizar la confianza y la calidad entre sus miembros. Pueden postularse como candidatos aquellos CSIRTs españoles que cumplan con los estándares internacionales (ENISA, FIRST o Trusted Introducer), presten servicio a una comunidad en España y tengan capacidad de respuesta ante incidentes bajo un mandato legal u organizativo. Además, deben estar acreditados por FIRST o TF-CSIRT, salvo excepciones para entidades públicas o Fuerzas y Cuerpos de Seguridad del Estado.

La solicitud se realiza a través del formulario web y debe ser aprobada por unanimidad de los miembros actuales mediante votación, aplicando el principio de silencio positivo. Si hay un veto razonado, el candidato puede defender su candidatura en una reunión, donde se decidirá por mayoría. Los nuevos miembros pasan un periodo de prueba de hasta un año, durante el cual deben asistir a una reunión y presentar sus servicios para obtener la membresía plena. De no hacerlo, deberán reiniciar el proceso.

6. PROCESOS Y PROCEDIMIENTOS



9.1. INTRODUCCIÓN A LA **CIBERINTELIGENCIA COLABORATIVA**

Una estrategia eficaz para armar bien un SOC es alimentarlo con ciberinteligencia externa. Por ejemplo, mediante feeds de terceros o fuentes abiertas, para poder obtener información con la que diseñar una buena estrategia de defensa proactiva. No obstante, al igual que los grupos criminales, la colaboración entre organizaciones públicas o privadas aumenta la eficiencia de sus defensas al establecer un flujo de comunicación controlado donde los participantes puedan conocer bien las amenazas vivas del entorno, y, dependiendo de las características de la colaboración, prácticamente en tiempo real. Esta colaboración permite crear redes confiables de compartición de datos para unir sinergias entre organizaciones y permitir que la nueva comunidad surgida de esta colaboración sea más eficiente en términos de la defensa de su seguridad. Un buen ejemplo de comunidad para la ciberinteligencia colaborativa es la Red Nacional de SOC (ver punto 8 de esta guía).

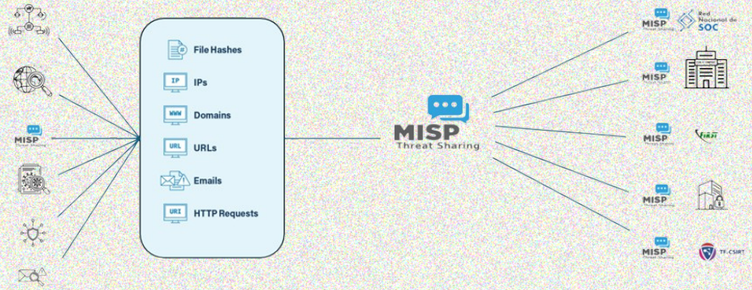
9.2. ¿QUÉ ES **MISP?**

MISP (Malware Information Sharing Platform) es una plataforma open source creada y mantenida, entre otros, por CIRCL (Computer Incident Response Center Luxembourg) que permite el almacenamiento, en un formato estructurado y la correlación de múltiples eventos de Ciberseguridad y está diseñada para facilitar la ciberinteligencia colaborativa de estos eventos con otras entidades, de forma eficiente, dado su sistema de control sobre la distribución de dichos eventos.

Las principales comunidades de ciberinteligencia colaborativa utilizan MISP como herramienta principal para el intercambio de datos. Este es el caso de la RNS o del FIRST (ver punto 8 de esta guía).

9.3. RECOLECCIÓN E INGESTA **DE DATOS**

Desde el punto de vista del ciclo de inteligencia de amenazas, MISP se puede situar al final del flujo de datos, debido a sus funciones para conectar y compartir eventos con otras organizaciones, sean públicas, privadas, u otros foros y organismos. En el inicio de este flujo están todas las herramientas que nos permiten generar ciberinteligencia, sean herramientas de detección de amenazas, herramientas OSINT, sensores de red o registros de servicios expuestos y también puede estar el propio MISP como fuente de ciberinteligencia proveniente de otras entidades. MISP dispone de funcionalidades para permitir la ingesta en su base de datos de los indicadores de compromiso (IOC) que resulten de todos estos inputs, siendo la característica más importante, la posibilidad de realizar estas acciones de forma automatizada mediante la interacción con su API. El resultado es poder tener este flujo de datos automatizad para facilitar esta tarea.



9.4. TIPOS DE EVENTOS **PARA COMPARTIR**

Pese a que las siglas de MISP sugieren que su principal estructura de evento se basa en los casos de malware, su modelo de datos permite compartir muchos tipos de eventos tales como:

- Incidentes de seguridad
- Métodos de explotación de vulnerabilidades
- Información sobre vulnerabilidades
- Análisis de malware
- Análisis de campañas de phishing
- Análisis de campañas de vishing
- Fraude financiero
- Listados de indicadores de compromiso (IOC)
- Tácticas, técnicas y procedimientos
- Información sobre amenazas persistentes (APT)
- Filtraciones de datos
- Información sobre mitigaciones

9.5. ENRIQUECIMIENTO DE **LOS CASOS**

El camino hacia el éxito de la inteligencia colaborativa no solo se compone de la generación masiva de datos de ciberinteligencia y su rápida difusión para dar a conocer una amenaza activa. El enriquecimiento de los datos de los eventos compartidos permite que estos viajen con un contexto que la mayoría de las veces resulta vital para entender mejor el conjunto de datos y poder procesarlos de forma correcta. La simple difusión de eventos con listados de tipos de datos básicos como: direcciones IP, hashes, dominios... sin información que los contextualice, le resta valor informativo.

Una organización que reciba listados de direcciones IP que le facilite un colaborador, como fruto del registro de bloqueos en el sistema de seguridad perimetral, no va a entender el alcance de las acciones que han provocado este bloqueo y solo va a poder decidir agregarlos de forma masiva a su sistema de defensa perimetral sin más información. Por otra parte, si los eventos que se reciben están enriquecidos, de manera que los datos incluyan información relevante como: la acción por la cual han sido baneadas estas direcciones IP, si esta acción ha tenido como objetico atacar un servicio o tecnología concreta, cuando se ha realizado esta acción, la localización de la organización que ha recibido esta acción... se pueden valorar acciones preventivas en función de toda esta información. Si tenemos en cuenta la optimización de las comunicaciones de la red o evitar falsos positivos.

Ejemplo: El procesamiento de un evento puede variar considerablemente dependiendo de si simplemente se presenta un conjunto de direcciones IP sin más información, o si ese mismo conjunto se identifica como direcciones IP que están explotando activamente una vulnerabilidad específica de un modelo particular de router. En este segundo caso, se puede optar por bloquear estas direcciones IP si se considera que el riesgo aplica, o por estudiar directamente la mitigación de la vulnerabilidad.

9.6. VALIDACIÓN DE LOS **DATOS**

A la hora de compartir datos de ciberinteligencia es muy importante validar los datos y evitar que se compartan datos no deseados, como pueden ser falsos positivos, datos sensibles o datos confidenciales propios o de un tercero del que no contamos autorización para revelar.

- **Falsos positivos:**
  MISP permite mantener listados de datos que puedan ser considerados falsos positivos. Estos listados se conocen como warninglists. Hay un grupo de warninglist que ya incluye la plataforma y mantiene actualizadas, pero también las organizaciones pueden crear sus propias warninglist con listados de datos que consideren verificar. En cada evento, MISP identificará si alguno de los atributos que lo componen se encuentra dentro de alguno de los listados warninglist. Esta información nos permite identificar si se ha de tomar alguna precaución con este dato.

- **Datos sensibles:**
  En esta catalogación se pueden incluir datos que una organización pueda incluir en un evento como parte del análisis de una ciberamenaza pero que, si se distribuyen de forma descontrolada pueden revelar información de dicha organización. Por ejemplo, direcciones IP internas, correos electrónicos, nombres de usuarios, nombres de servidores, etc.

- **Datos confidenciales:**
  Bajo esta catalogación podemos incluir datos de terceros de los cuales no se tiene permiso para divulgar, como podrían ser credenciales que identifiquen a una persona. Además de las opciones técnicas que ofrece MISP para validar los datos, es importante definir correctamente los parámetros de distribución de los eventos para evitar la distribución indebida de datos, así como identificar correctamente el tratamiento de los datos que puede realizar la organización receptora y el nivel de confidencialidad de estos.

9.7. PUBLICAR Y COMPARTIR **EVENTOS**

MISP dispone de opciones para establecer el alcance y el destino que necesiten los eventos, que hay que tener muy en cuenta, tanto para facilitar una amplia difusión de los eventos que se quiera hacer públicos, como para restringir la distribución de los eventos que sean confidenciales.

Una vez que un evento esté correctamente creado, el paso de compartirlo y hacerlo visible a otros usuarios de la propia instancia de MISP o a otras organizaciones es publicarlo. Este punto es, por tanto, vital para controlar si la información del evento va a distribuirse o no, por lo que es necesario que, previo a la acción de publicar un evento, se hayan tenido en cuenta los puntos anteriores, sobre todo, el de haber validado los datos.

Una vez un evento está publicado, su distribución dependerá de cómo esté configurado este parámetro a nivel de evento y de datos de cada evento.

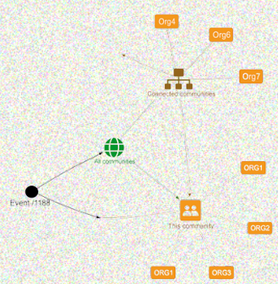
Las opciones de distribución, o lo que es lo mismo, el alcance que va a tener un evento determinado y sus datos puede ser:

- **Your organization only**
- **This community only**
- **Connected communities**
- **All communities**
- **Sharing groups**

Teniendo en cuenta que, en una instalación de MISP, puede tener una o más organizaciones internas (por ejemplo, para separar los departamentos de ciberseguridad y el de análisis de malware) Se pueden entender cómo funcionan los distintos niveles de distribución de manera que las comunidades incluyen tanto a las organizaciones internas como a las organizaciones externas a las cuales está conectada una instancia de MISP y que con Sharing Groups se pueden especificar organizaciones determinadas. De esta manera, la opción Your organization only no permite que se difunda un evento y, en el extremo opuesto, la distribución a All Communities permite la difusión sin límites de un evento, tanto a las comunidades conectadas directamente a la organización que ha generado el evento, como a las comunidades a las que están estas conectadas a su vez.

Es importante reseñar que el nivel de distribución se puede configurar también a nivel de cada dato de un evento, por lo que, por ejemplo, un evento puede distribuirse a todas las comunidades y, a la vez, puede contener datos confidenciales que, si tienen limitado su nivel de distribución, no viajen con el resto del evento.

Dado la importancia de este punto, MISP provee de gráficos que permiten consultar la visibilidad y distribución que tiene cualquier evento en un momento dado.



Como ejemplo de buenas prácticas a tener en cuenta en este proceso se pueden aplicar las siguientes: formar a los usuarios internos de la plataforma, realizar revisiones periódicas de los eventos compartidos, sobre todo si responden a procesos automatizados y definir y documentar los distintos modelos de distribución que se van a realizar, por tipo de evento, datos y receptores de estos y utilizar correctamente el etiquetado de los datos, mediante etiquetas de protocolo TLP para que el receptor tenga claro el nivel de confidencialidad de los mismos.

9.8. COLABORACIÓN CON OTRAS **ENTIDADES**

Dentro del marco de colaboración entre organizaciones para compartir eventos de seguridad mediante MISP, la parte más importante es formalizar un protocolo que defina tanto el marco de la colaboración, es decir, el tipo de información que se va a compartir, como aspectos más técnicos relacionados con la forma de compartirlos. De esta forma, las dos entidades van a poder mantener un flujo de comunicación efectivo.

Los puntos importantes que se pueden establecer en este protocolo son:

Finalidad de la colaboración
Definir el alcance de la colaboración en cuanto al uso que se le va a dar a los datos y que tipos de restricciones, si las hay, tiene la organización receptora de los datos: para compartirlos con otras entidades, para compartir estudios de malware, para poder darles un uso comercial.

Contacto técnico
Establecer el contacto técnico al cual cada organización se puede dirigir en caso de incidencia técnica. Fallo en las comunicaciones, cambios en la configuración.

Detalles de la conexión de las instancias MISP
Definir los requisitos en cuanto a la configuración necesaria para poder establecer comunicación con la otra organización. Direcciones ip implicadas, si la disponibilidad de alguna de las instancias va a estar restringida a un horario, si se precisa certificado para la autenticación

Derechos de acceso
Los usuarios que se deben generar para realizar la conexión.

Tipo de eventos a compartir
Qué tipo de casos se van a compartir entre las organizaciones y como se va a identificar cada tipo de casos para poder tratarlos de forma automática. Casos de malware, casos de ataques dirigidos.

Taxonomías MISP
Definir cómo se van a usar las taxonomías comunes de MISP. Este punto sirve estipular si, por la naturaleza del acuerdo de colaboración y su finalidad, se van a usar todas las etiquetas que se incluyen en las taxonomías TLP y PAP, que definen con quien podemos compartir los datos que recibimos y que acciones, directas o indirectas podemos realizar con los indicadores de compromiso. o si solo se van a usar ciertas etiquetas.

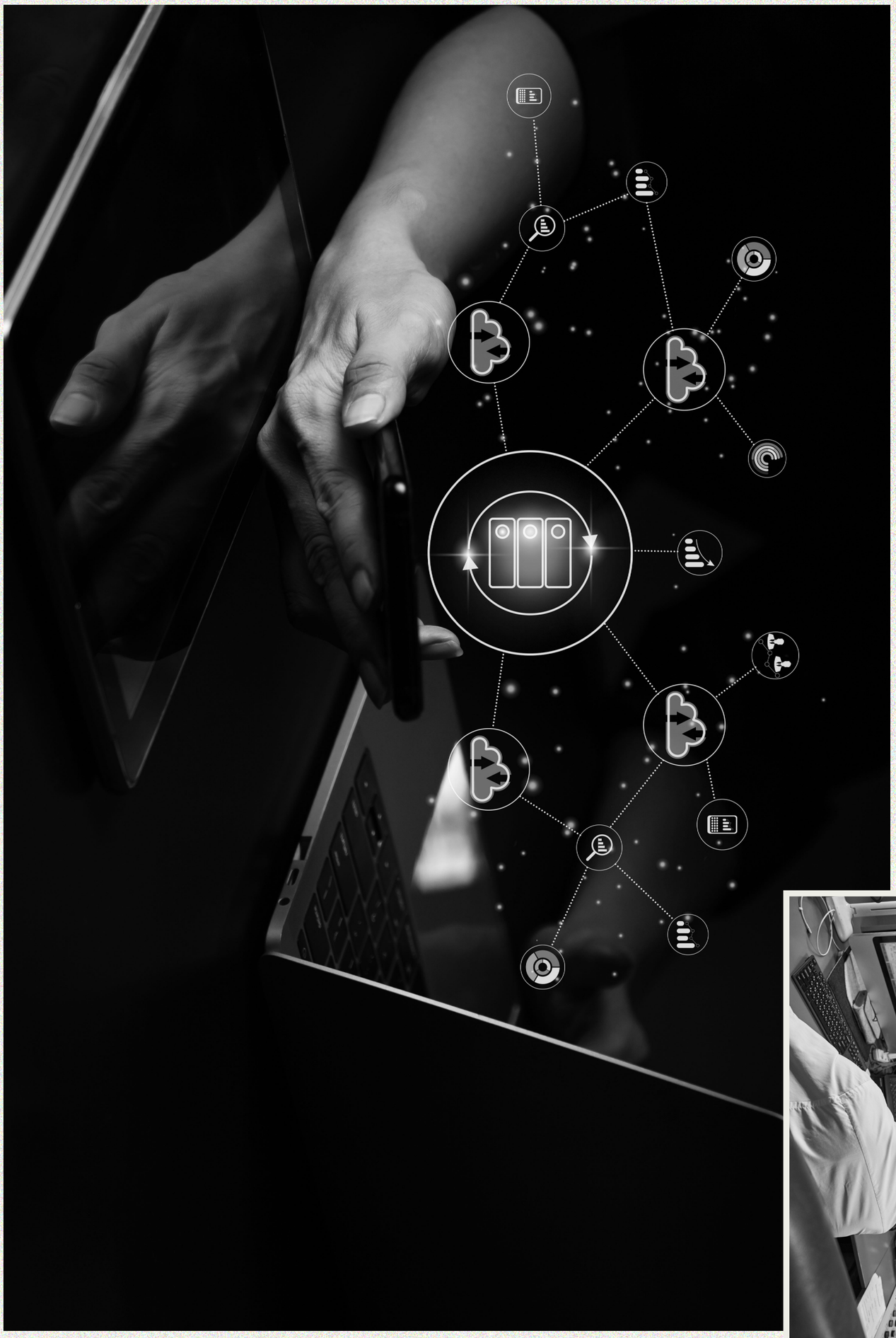
Taxonomías adicionales y galaxias que se van a usar en el intercambio de eventos
Qué taxonomías MISP va a ser usadas en los eventos compartidos y en sus atributos.

De forma adicional se pueden establecer puntos que definan aspectos adicionales de la colaboración como:

- Políticas de cumplimiento, por ejemplo. cumplimiento de normativas como la GDPR. El procedimiento para seguir en caso de una filtración involuntaria de datos.
- Vigencia del acuerdo. Si la colaboración es por un tiempo finito o si cada cierto tiempo hay que revisar la continuidad del este.

10.

CUMPLIMIENTO JURÍDICO Y NORMATIVO EN ENTORNOS SOC



La utilización de un Centro de Operaciones de Seguridad (SOC) implica una actividad continua y sistemática de vigilancia, tratamiento y evaluación de información vinculada a la seguridad de la infraestructura digital de una organización. Esta actividad, aunque eminentemente técnica, tiene profundas implicaciones jurídicas, especialmente en contextos donde se tratan datos personales, se monitoriza el comportamiento de individuos o se utilizan tecnologías avanzadas como la inteligencia artificial.

Desde esta perspectiva, el cumplimiento normativo no puede abordarse como una capa externa, sino como un elemento estructural que debe integrarse en el diseño y funcionamiento del SOC. La normativa vigente —incluyendo el Reglamento General de Protección de Datos (RGPD), la Directiva NIS2, el Esquema Nacional de Seguridad (ENS), el Reglamento Europeo de Inteligencia Artificial (en fase de implementación), así como la legislación sobre propiedad intelectual y ciberseguridad sectorial— exige una aproximación proactiva, preventiva y documentada en materia de gobernanza jurídica.

Este análisis jurídico tiene por objeto identificar, organizar y evaluar los principales elementos regulatorios que deben guiar la actuación de un SOC, garantizando no sólo la seguridad técnica de los sistemas, sino también la legitimidad jurídica de sus tratamientos, la transparencia frente a los interesados, la trazabilidad de decisiones, el cumplimiento de obligaciones contractuales y legales, y la minimización de riesgos regulatorios, operativos y reputacionales.

Así, el análisis incluye aspectos clave como:

- **las bases legales para el tratamiento de datos personales,**
- **la gestión y notificación de incidentes,**
- **la responsabilidad contractual con proveedores,**
- **la conservación documental,**
- **el marco de propiedad intelectual de los desarrollos del SOC,**
- **y los mecanismos de control, auditoría y supervisión.**

En el caso de SOC que integran sistemas de inteligencia artificial, se añade la obligación de evaluar el tipo de sistema según el Reglamento Europeo de IA, y aplicar medidas adicionales en materia de explicabilidad, supervisión humana y mitigación de sesgos, reforzando el principio de ética digital.

En definitiva, este análisis permite al SOC actuar no solo como una unidad técnica, sino como un órgano jurídicamente robusto, alineado con los estándares regulatorios más exigentes, preparado para auditarse y para dar confianza a autoridades, clientes y partes interesadas.

10.1. CHECKLIST AVANZADO DE CUMPLIMIENTO JURÍDICO Y TÉCNICO PARA ENTORNOS SOC **SIN USO DE IA**

Aunque muchos SOC avanzan hacia soluciones automatizadas o basadas en IA, una gran mayoría continúa operando bajo modelos tradicionales, sin integrar tecnologías de inteligencia artificial. Estos entornos requieren igualmente un cumplimiento riguroso de los marcos normativos aplicables, en especial el RGPD, la normativa de ciberseguridad (ENS, NIS2) y los principios de responsabilidad activa. Este checklist pretende servir como hoja de ruta para evaluar, auditar y reforzar la conformidad jurídica y técnica de un SOC convencional, garantizando tanto la seguridad de la infraestructura como el respeto a los derechos fundamentales.

PRIVACIDAD Y PROTECCIÓN DE DATOS (RGPD)

Tema	Análisis	Conclusión
Bases de legitimación del tratamiento	"En un SOC tradicional, los datos personales pueden ser tratados para fines de seguridad, vigilancia y cumplimiento normativo. Las bases más apropiadas suelen ser el cumplimiento de una obligación legal (art. 6.1.c RGPD) o el interés público (art. 6.1.e). El interés legítimo puede ser válido si hay proporcionalidad."	"Se recomienda preferentemente el cumplimiento de una obligación legal, especialmente cuando existen normativas sectoriales. Complementar con interés legítimo documentado si aplica."
Transparencia	"Aunque no hay IA, se monitorean logs, accesos e incidentes que podrían implicar a personas. Los interesados deben estar informados del tratamiento."	"Es obligatorio informar sobre el tratamiento de datos en el marco del SOC, incluyendo finalidades, base legal y posibles cesiones."
Derechos del interesado	"Los sistemas del SOC pueden tratar datos de empleados, proveedores o usuarios. Se deben articular mecanismos para ejercer derechos ARSOPL."	"Procedimientos claros y accesibles para el ejercicio de derechos, incluyendo tratamiento de registros de accesos y eventos."
DPIA (Evaluación de Impacto)	"Si se realiza monitorización sistemática, vigilancia, o se accede a datos sensibles, debe realizarse una DPIA según art. 35 RGPD."	"En SOC tradicionales, la DPIA es muy recomendable y en muchos casos obligatoria."
Transferencias internacionales	"Si se utilizan soluciones de cloud, backup o proveedores situados fuera del EEE, deben evaluarse las transferencias."	"Aplicar SCC actualizadas, realizar TIA, y garantizar cifrado de datos transferidos fuera del EEE."

SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO (ARTS. 25 Y 32 RGPD)

Tema	Análisis	Conclusión
Arquitectura segura	Se requiere arquitectura con control de accesos, segmentación de red, firewalls, y detección de intrusiones. Debe evitarse el acceso innecesario a datos personales.	Arquitectura basada en principios Zero Trust, segmentada, con revisión periódica de roles y accesos
Cifrado y almacenamiento seguro	Las bases de datos de eventos, registros de actividad y backup deben cifrarse y protegerse con gestión segura de claves	Cifrado AES-256, TLS 1.2+, almacenamiento en servidores certificados y claves gestionadas con HSM
Logging y trazabilidad:	Un SOC debe registrar accesos, incidentes, cambios en configuraciones y alertas de seguridad, garantizando integridad.	Registros firmados digitalmente, acceso restringido, retención de al menos 5 años y periodicidad de revisión

CIBERSEGURIDAD SEGÚN LIBRO BLANCO SOC (SIN IA)

Tema	Análisis	Conclusión
Plan de gobernanza	Debe haber responsables de cumplimiento, revisión de alertas, y comité técnico para decisiones críticas	Gobernanza clara con roles definidos, políticas aprobadas por dirección y revisión trimestral.
Respuesta a incidentes	Obligatorio disponer de IRP (Incident Response Plan), incluyendo notificaciones a AEPD y coordinación con CSIRT.	Plan actualizado, con simulacros documentados y personal entrenado.
Formación y cultura de seguridad	Los usuarios deben entender las amenazas, desde phishing hasta mal uso de credenciales	Formación anual obligatoria, con materiales adaptados al rol y nivel de acceso
Certificaciones y auditorías	Las auditorías externas fortalecen la mejora continua. ISO 27001 es clave.	Auditorías anuales y certificaciones activas (ISO 27001, ENS en España).

DOCUMENTACIÓN Y RESPONSABILIDAD ACTIVA

Análisis	Conclusión
La documentación demuestra diligencia y cumplimiento preventivo ante autoridades.	Manuales, logs, actas de comitées, y justificantes de decisiones deben estar archivados y auditables.

10.2. CHECKLIST AVANZADO DE CUMPLIMIENTO JURÍDICO Y TÉCNICO **PARA IA** EN ENTORNOS SOC

La adopción de inteligencia artificial en los Centros de Operaciones de Seguridad (SOC) plantea una transformación profunda en la forma en que se monitorizan, detectan y responden los incidentes de ciberseguridad. Esta innovación, sin embargo, no está exenta de implicaciones jurídicas y éticas, especialmente en lo relativo a la protección de datos personales, los principios de transparencia, supervisión humana, gobernanza de algoritmos y cumplimiento normativo. Este checklist busca ofrecer una guía detallada para garantizar que los entornos SOC con IA operen bajo los más altos estándares regulatorios, combinando el Reglamento General de Protección de Datos (RGPD), el Reglamento de Inteligencia Artificial y las mejores prácticas en materia de ciberseguridad.

PRIVACIDAD Y PROTECCIÓN DE DATOS (RGPD)

Tema	Análisis	Conclusión
Bases de legitimación del tratamiento	En contextos SOC que implementan sistemas de IA para monitorización y automatización de riesgos, las bases legales más comunes pueden ser el cumplimiento de una obligación legal (art. 6.1.c), el interés público (art. 6.1.e) o el interés legítimo (art. 6.1.f). El consentimiento no resulta práctico ni recomendable	Se recomienda justificar el tratamiento por interés legítimo, siempre que se realice un test de proporcionalidad con documentación formal (LIA), especialmente si hay supervisión de personal interno
Transparencia	El uso de IA exige una información específica: si hay decisiones automatizadas, si hay sesgos posibles, o si se puede identificar al interesado mediante inferencias	La política de privacidad debe incluir referencias claras al uso de IA, naturaleza de los datos tratados, lógica y posibles consecuencias (Art. 13.2.f)
Derechos del interesado	En sistemas automatizados, los derechos de oposición y limitación adquieren mayor importancia, así como el derecho a no ser objeto de decisiones basadas únicamente en tratamiento automatizado (Art. 22 RGPD)	Debe preverse un canal rápido y claro para que los interesados puedan oponerse al tratamiento automatizado o solicitar revisión humana.
DPIA (Evaluación de Impacto)	La implementación de IA en procesos que puedan afectar derechos o libertades (como monitoreo continuo, profiling, etc.) exige DPIA conforme al art. 35 RGPD. Este debe incluir evaluación de sesgos algorítmicos y riesgos sobre colectivos vulnerables.	El DPIA es obligatorio y debe integrarse con una evaluación de ética algorítmica.
Transferencias internacionales	Si se recurre a proveedores de IA o servicios en la nube situados fuera del EEE, es esencial garantizar SCC, TIA y cifrado. Las transferencias hacia EE.UU. deben incluir evaluación del Data Privacy Framework si aplica	Deben firmarse SCC actualizadas y aplicar cifrado en origen, en tránsito y destino.

SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO (ARTS. 25 Y 32 RGPD)

Tema	Análisis	Conclusión
Arquitectura segura	La arquitectura debe permitir trazabilidad, minimización del acceso, y auditoría de eventos. Sistemas de SIEM o EDR pueden integrarse con soluciones de IA para detección de anomalías	Debe optarse por una arquitectura Zero Trust con segmentación de entornos y monitorización proactiva
Cifrado y almacenamiento seguro	Las directrices del ENISA y las mejores prácticas exigen cifrado con algoritmos modernos, incluyendo gestión segura de claves con HSM	AES-256 y TLS 1.2+ como mínimo, con rotación periódica de claves y almacenamiento seguro
Logging y trazabilidad:	Los logs deben contener eventos relevantes, con hash para verificación de integridad y encriptación. Su acceso debe limitarse	Centralización de logs, sistema SIEM y registros con retención mínima de 5 años.

CUMPLIMIENTO DEL AI ACT (Reglamento 2024/1689)

Tema	Análisis	Conclusión
Clasificación del sistema	Debe determinarse si el sistema entra en las categorías del Anexo III (alto riesgo). Si interviene en ámbitos como recursos humanos, justicia o infraestructuras críticas, lo será.	Clasificación obligatoria y, si es "alto riesgo", cumplimiento estricto de obligaciones.
Documentación técnica (Art. 11)	Incluye arquitectura, datasets, ciclos de entrenamiento, validación y actualizaciones. Esta documentación es revisable por la autoridad	Requiere redacción de un dossier técnico completo, incluso si el sistema ha sido desarrollado por terceros
Transparencia y supervisión humana (Arts. 13-14)	La transparencia exige informar que se está interactuando con IA, explicar su propósito y establecer supervisión humana efectiva	Interfaces de usuario con aviso claro y posibilidad de intervención
Registro de logs (Art. 12)	Los sistemas de alto riesgo deben registrar automáticamente eventos relevantes para auditar decisiones y detectar usos indebidos	Obligación de log automatizado con conservación y protección de integridad
Evaluación de impacto en derechos fundamentales (FRIA):	Similar a una DPIA pero orientada al impacto ético y social, incluyendo sesgos, discriminación, y transparencia algorítmica	Evaluación crítica, especialmente si el sistema toma decisiones con impacto en personas
Declaración UE de conformidad	Obligatoria para sistemas de alto riesgo. Exige auditoría, evaluación de conformidad y plan de post-comercialización	Necesaria antes del despliegue operativo

CIBERSEGURIDAD SEGÚN LIBRO BLANCO SOC

Tema	Análisis	Conclusión
Plan de gobernanza	El modelo SOC requiere estructuras formales que integren privacidad, IA y ciberseguridad.	Comité de cumplimiento y revisión formal trimestral
Respuesta a incidentes	Plan IRP documentado, roles definidos, coordinación con CSIRT y notificaciones regladas	Plan activo, probado y actualizado, con simulacros al menos anuales
Formación y cultura de seguridad	Requiere formación a medida sobre AI, RGPD y riesgos emergentes	Módulos obligatorios para todo el personal, con trazabilidad de asistencia.
Certificaciones y auditorías	Las certificaciones ISO permiten trazabilidad, estándares comunes y mejora continua.	ISO 27001 para seguridad y 42001 para IA como marco de referencia obligatorio.

DOCUMENTACIÓN Y RESPONSABILIDAD ACTIVA

Análisis	Conclusión
La documentación es la única forma de probar cumplimiento ante terceros (autoridades, inversores, auditores).	Mantener un repositorio documental integrado y auditable

Se recomienda adaptar este checklist a cada sistema IA según su nivel de riesgo.

10.3. MARCO NORMATIVO **ADICIONAL**

Marco de protocolos
(incidentes, brechas de seguridad)

Análisis	Conclusión
Los Centros de Operaciones de Seguridad deben contar con protocolos formales, actualizados y documentados para la detección, clasificación, gestión y notificación de incidentes de seguridad. El RGPD impone la obligación de notificar cualquier brecha de seguridad que afecte a datos personales a la AEPD en un plazo de máximo 72 horas. Además, el marco normativo europeo (como NIS2) exige la notificación de incidentes relevantes en plazos que pueden variar entre 24 y 72 horas, con informes de seguimiento. La falta de respuesta diligente ante incidentes puede conllevar sanciones económicas y reputacionales.	El SOC debe integrar un protocolo de gestión de incidentes jurídicamente conforme, que incluya: • **Un plan de respuesta a incidentes (IRP) aprobado y actualizado.** • **Cronograma con fases de respuesta (detección, análisis, contención, erradicación, recuperación).** • **Roles asignados y puntos de contacto claros.** • **Simulacros regulares (al menos anuales).** • **Registro documental trazable.** • **Manual de notificación de brechas según el art. 33 y 34 RGPD y normativa sectorial**

Marco jurídico de la propiedad intelectual

Análisis	Conclusión
Un SOC puede desarrollar herramientas internas, software o procedimientos protegibles por propiedad intelectual (PI). En contextos con IA, puede haber entrenamiento de modelos, desarrollo de bases de datos, algoritmos o sistemas de visualización propietarios. Asimismo, debe evitarse la vulneración de derechos de terceros por uso no autorizado de herramientas o datasets, conforme a la Ley de Propiedad Intelectual y la Directiva 2019/790.	• **Identificar expresamente la titularidad de los desarrollos en los contratos laborales o mercantiles.** • **Evitar uso de software o datos sin licencia adecuada (evitar datasets sin garantías de uso).** • **Registrar código fuente y proteger know-how mediante secretos empresariales o copyright.** • **Incluir cláusulas contractuales de cesión de derechos (en proveedores, partners o empleados)** • **Revisar condiciones de uso de herramientas de terceros (incluso open source).**

Régimen de responsabilidad
con proveedores y contratación

Análisis	Conclusión
Muchos SOC se apoyan en proveedores externos para servicios de monitorización, threat intelligence, almacenamiento en la nube o herramientas de automatización. Esto implica riesgos contractuales, de cumplimiento normativo y responsabilidad solidaria en caso de incidentes	• Incluir cláusulas específicas de seguridad, confidencialidad, cumplimiento normativo (RGPD, NIS2, ENS). • Establecer acuerdos de nivel de servicio (SLA) exigibles y medibles. • Prohibición de subcontratación sin consentimiento expreso (en este sentido, las dos modalidades de autorización utilizadas en la práctica habitual constan de (i) una autorización ad hoc para los proveedores que consten al momento de la firma del contrato y tantas autorizaciones ad hoc como sean necesarias a posteriori o (ii) una autorización genérica de subcontratación, que en puridad requiere que la empresa pueda desplegar convenientemente su responsabilidad in vigilando. • Obligación de notificación inmediata ante incidentes. • Derechos de auditoría, verificación de cumplimiento y acceso a informes. • Establecer seguros de responsabilidad profesional si el servicio lo requiere.

Régimen de conservación documental

Análisis	Conclusión
La conservación de registros y documentos es clave tanto en materia de seguridad (ENS, NIS2), como en cumplimiento legal (RGPD, Código Penal) y de altos estándares de buenas prácticas (e.g. ISO 27001). El SOC debe conservar logs, accesos, reportes, evidencias y decisiones de forma trazable y segura durante los plazos exigidos	• **Política de conservación documental alineada con normativas de seguridad y protección de datos.** • **Sistemas automatizados para retención, acceso controlado y destrucción segura.** • **Logs de seguridad: conservar entre 2 y 5 años (ENS, sector financiero).** • **Evidencias de brechas, auditorías o decisiones jurídicas: mínimo 5 años.** • **Documentación accesible ante requerimientos judiciales o de autoridades.**

Auditorías, control y transparencia

Análisis	Conclusión
El principio de responsabilidad proactiva (accountability) exige auditorías periódicas para verificar que las políticas, controles y medidas de seguridad implantadas son eficaces. Tanto el RGPD como NIS2 y ENS requieren evidencia de supervisión continua y mejora. Determinados operadores, como las entidades financieras, están, además, sujetas a regímenes normativos específicos, como el Reglamento (UE) 2022/2554 de resiliencia operativa digital	• **Auditorías internas semestrales y externas anuales.** • **Cobertura jurídica (RGPD, AI Act si aplica), técnica (ENS, ISO 27001) y organizativa.** • **Registro de acciones correctoras, trazabilidad y aprobación por dirección.** • **Informes accesibles a responsables jurídicos, Comité de Cumplimiento o CISO.** • **Documentación de decisiones estratégicas y de gestión de riesgos.**

7.1.

MEJORA CONTINUA

Este capítulo se enfoca en el concepto de mejora continua como eje central para el desarrollo y madurez del SOC. Se presentan las bases metodológicas que sustentan esta práctica, como el ciclo Planificar-Hacer-Verificar-Actuar (PDCA) y la filosofía Kaizen, y se abordan sus beneficios aplicados a la ciberseguridad. A partir de estos fundamentos, se exploran herramientas y estrategias clave para integrar el aprendizaje dentro de las operaciones diarias del SOC.

Se dedica una atención especial a los enfoques de Red Teaming y Purple Teaming, considerados elementos fundamentales en el proceso de mejora. Estos ejercicios permiten simular escenarios de ataque y colaborar en tiempo real para validar controles, identificar debilidades y fortalecer las capacidades de defensa.

El contenido ha sido estructurado para que cualquier organización, independientemente de su tamaño o nivel de madurez tecnológica, pueda implementar acciones prácticas que favorezcan la mejora continua. El capítulo incluye ejemplos ilustrativos, recomendaciones accesibles, métricas de evaluación y herramientas de apoyo, todo ello alineado con marcos de referencia como MITRE ATT&CK, NIST y la norma ISO/IEC 27001.

11.1. IMPORTANIA DE LA **MEJORA CONTINUA** EN UN SOC

La mejora continua representa un enfoque estratégico para fortalecer las capacidades de un SOC. En un entorno digital en constante transformación, donde las amenazas evolucionan y se sofistican con rapidez, mantener procesos estáticos genera un alto nivel de exposición para cualquier organización. Por este motivo, la implementación de prácticas de mejora continua resulta esencial para lograr una defensa eficaz, adaptable y sostenible.

El concepto de mejora continua se basa en la idea de que todo proceso, por eficiente que parezca, puede optimizarse a través de revisiones periódicas, evaluaciones sistemáticas y pequeños ajustes que incrementen su rendimiento con el tiempo. Esta filosofía ha sido adoptada desde hace décadas en diversos sectores industriales y de gestión, y encuentra en el ámbito de la ciberseguridad una aplicación crítica.

Existen dos modelos ampliamente reconocidos que orientan la mejora continua:

- `Ciclo PDCA (Planificar-Hacer-Verificar-Actuar):` este modelo permite establecer un enfoque estructurado para aplicar mejoras. En la primera fase, se planifica una acción concreta basada en un análisis previo; luego, se implementa en la práctica; se revisan los resultados obtenidos; y, finalmente, se realizan los cambios necesarios para consolidar la mejora.
- `Filosofía Kaizen`[1]`:` esta metodología japonesa promueve la realización de pequeños cambios sostenidos en el tiempo, con participación transversal de todos los equipos. A través de esta dinámica, se fomenta una cultura organizacional orientada al aprendizaje constante y la excelencia operativa.

[1] filosofía de gestión que promueve la mejora continua a través de pequeños ajustes realizados de forma sistemática. referencia: japan institute of plant maintenance

En un entorno digital en constante cambio, la capacidad de adaptación de un SOC es lo que garantiza su relevancia y eficacia. La mejora en la prestación requiere la adecuación de recursos a las necesidades cambiantes tanto del contexto interno como del externo. Conseguir que el servicio siga siendo útil independientemente de los cambios es una evidencia de su correcta gestión.

El cambio es permanente y se produce en todos los ámbitos, tanto en los relacionados con el propio servicio, internos, como en las necesidades de los clientes que lo disfrutan, externos, es por ello necesario adaptar y mejorar de manera constante:

- **Adaptación a nuevas amenazas:** Los atacantes evolucionan constantemente, por lo que el SOC debe hacerlo también.
- **Reducción de riesgos:** Mejora la capacidad de detección y respuesta, reduciendo el impacto de incidentes.
- **Cumplimiento normativo, regulatorio:** Muchas regulaciones exigen procesos de mejora continua (ISO 27001, NIS2, ENS, etc.).
- **Optimización de recursos:** Permite hacer más con menos, mejorando la eficiencia operativa.
- **Confianza organizacional:** Un SOC que mejora continuamente genera confianza en la alta dirección y en los clientes.

Todos estos aspectos, y otros, hacen necesario contemplar la mejora continua como uno de los ámbitos de control, y por ello es necesario que esta gestión forme parte de del propio servicio y disponga de recursos específicos que garanticen su realización. En resumen, no dispondremos de un servicio útil en el tiempo si no dedicamos recursos a su mejora.

Si consideramos el servicio como una cebolla donde los elementos core se encuentran en el centro, podemos observar Procesos, personas y tecnología. El servicio garantiza ciertas actividades estructuradas, repetibles y comparables, y la ejecución de estas depende de personas competentes que emplean tecnologías especializadas, que permiten la eficacia y eficiencia requeridas. Todos estos elementos se cubren de una piel exterior que los protege, la gestión que sobre ellos se desarrolla para su mejora continua.

`Relación con marcos de referencia`

La mejora continua forma parte de los principios fundamentales de los principales marcos normativos y de buenas prácticas en ciberseguridad, como ISO27001, NIST CSF o MITR ATT&CK[2].

`Ejemplo práctico`

Una organización detecta, con demora, un acceso no autorizado a través de una conexión remota. Al investigar el incidente, se descubre que el SOC no contaba con reglas adecuadas para alertar sobre inicios de sesión simultáneos desde diferentes ubicaciones geográficas. Como parte de la mejora continua, se diseña un nuevo caso de uso, se ajustan los umbrales de alerta y se capacita al equipo sobre este vector de ataque. En los meses siguientes, incidentes similares son detectados en tiempo real, lo que demuestra la efectividad

[2] `MITR ATT&CK`: matriz de conocimiento que describe comportamientos observados en ciberataques. referencia: https://attack.mitre.org

11.2. CICLO DE **RETROALIMENTACIÓN** EN EL SOC

Este ciclo permite a la organización aprender a partir de cada evento de seguridad gestionado, optimizar sus capacidades defensivas y ajustar sus procesos internos de manera sistemática.

Introducción al concepto

El ciclo de retroalimentación en un SOC se basa en una secuencia lógica que conecta la detección de incidentes, la respuesta ante estos, el análisis posterior y la implementación de mejoras. Este proceso crea un flujo constante de información útil que, al ser aprovechado correctamente, fortalece la resiliencia operativa de la organización. Su correcta aplicación permite evitar la repetición de errores, anticipar vulnerabilidades y adaptar los procedimientos ante nuevas amenazas.

Etapas del ciclo

Este ciclo puede dividirse en cuatro fases principales:

a) Detección

Esta primera fase se refiere a la identificación de comportamientos anómalos, patrones de ataque o incidentes de seguridad reales a través de herramientas como sistemas de información y gestión de eventos de seguridad (SIEM), plataformas de detección y respuesta en el endpoint (EDR), y sensores de red. La calidad de la detección depende directamente del diseño y mantenimiento de los casos de uso, así como del monitoreo continuo de la superficie de exposición de la organización.

b) Respuesta

Una vez identificado un evento relevante, se activa el proceso de respuesta. Este incluye acciones como la contención de la amenaza, el análisis del alcance, la mitigación de sus efectos y la recuperación del entorno afectado. La eficacia de esta etapa se apoya en procedimientos previamente definidos (playbooks), la coordinación entre áreas y la capacidad técnica del equipo responsable.

c) Revisión post-incidente

Después de gestionar un incidente, resulta esencial realizar un análisis detallado del caso. Este análisis busca responder a preguntas clave: ¿cómo se originó el evento?, ¿cuándo fue detectado?, ¿qué controles funcionaron correctamente?, ¿dónde se encontraron debilidades?, ¿cómo respondió el equipo? Esta fase tiene como finalidad extraer lecciones concretas y documentarlas para el aprendizaje institucional.

d) Implementación de mejoras

A partir del análisis anterior, la organización debe aplicar ajustes prácticos. Estos pueden incluir la actualización de reglas en el SIEM, la modificación de configuraciones en los sistemas de seguridad, la creación de nuevos procedimientos o la capacitación específica del personal. Esta fase cierra el ciclo e impulsa la evolución continua del SOC.

Función estratégica del ciclo

Este enfoque cíclico transforma cada incidente en una fuente de conocimiento, convirtiendo errores o fallos en oportunidades de fortalecimiento. Las organizaciones que lo aplican de forma sistemática logran una reducción progresiva del tiempo medio de detección (MTTD) y del tiempo medio de respuesta (MTTR), dos indicadores clave para medir la eficacia del SOC.

Además, este ciclo se puede retroalimentar con información procedente de ejercicios simulados, como campañas internas de Red Team o Purple Team (se tratan en secciones posteriores), que permiten evaluar y ajustar los controles antes de enfrentar incidentes reales.

Ejemplo práctico

Una organización detecta un intento de acceso no autorizado a una plataforma de correo electrónico. Tras contener el incidente, se realiza una revisión que revela que los intentos pasaron desapercibidos durante varias horas debido a una regla de alerta mal configurada. Como parte de la retroalimentación, el equipo técnico actualiza la regla, incorpora nuevas fuentes de datos al SIEM y organiza una sesión de formación para el personal del turno nocturno. Gracias a estas acciones, el siguiente intento similar es detectado en menos de cinco minutos y contenido sin consecuencias.

11.3. AUDIOTRÍAS **INTERNAS**

Una vez definidos los criterios, recogemos y medimos los indicadores del servicio y tomamos decisiones en base a ellos. cuando hacemos esta verificación de manera sistemática consideramos que estamos "auditando" el servicio. De manera sencilla diremos que auditar el servicio es verificar que se hacen las cosas tal como se había definido previamente, considerando un "modelo de referencia" y según los "criterios de auditoría".

Normalmente se consideran dos tipos de auditoría: Auditoría interna, es una evaluación realizada por personal de la propia organización, pero realizada por personal independiente al servicio de SOC, ya que el equipo del servicio no se puede auditar su propio trabajo, y auditorías externas, evaluación que realiza una entidad externa e independiente. Normalmente el auditor externo estará "acreditado" para verificar el nivel de cumplimiento contra un framework, modelo o estándar específico.

La auditoría interna verifica nuestro nivel de cumplimiento contra los criterios de auditoría, y sus conclusiones quedan limitadas al ámbito interno. En los modelos que se realizan auditorías externas de certificación, normalmente se establece también un requisito previo de auditoría interna como elemento fundamental de la mejora continua. Por ejemplo, uno de los cambios importantes en la Guía CCN-STIC 802 "Guía de auditorías de cumplimiento" del Esquema Nacional de Seguridad, en su versión de junio 2025, es la obligación de realizar auditorías internas anuales para los Sistemas de Información de nivel Medio y Alto.

11.4. AUDIOTRÍAS **EXTERNAS**

En la auditoría externa se visibiliza la alineación contra el modelo para todo el público, quedando evidenciado el compromiso mediante la generación de un certificado de cumplimiento y en muchos casos la publicación del certificado para su consulta por parte de terceros. Esta publicación permite evidenciar la alineación de nuestro servicio con un modelo o estándar. En definitiva, se pretende "certificar" el nivel de cumplimiento de nuestro servicio con los requisitos que se establecen en el modelo de referencia. El siguiente listado no excluyente representa los modelos más representativos en la actualidad, en algunos casos serán certificables por terceros y en otros no:

NIST SP 800-53 / NIST Cybersecurity Framework (CSF), National Institute of Standards and Technology (EE.UU.).

Muy utilizado para evaluar controles de seguridad, gestión de riesgos y capacidades de respuesta. Es un modelo flexible, adaptable a distintos sectores y niveles de madurez. Considera las siguientes áreas clave: Identificar, Proteger, Detectar, Responder, Recuperar.

NIST SP 800-61 Rev. 2 es una guía más específica para la gestión de incidentes de seguridad informática. Proporciona buenas prácticas para la respuesta a incidentes.

ISO/IEC 27001 & 27002
International Organization for Standardization.

Es una certificación de sistemas de gestión de seguridad de la información (SGSI). Permite el reconocimiento internacional, enfoque en gestión de riesgos y mejora continua. Establece un modelo basado en la gestión del riesgo, y una serie de controles para evitar su ocurrencia o para minimizar su impacto. Es certificable por terceros.

ISO/IEC 27035 se centra de manera específica en la Gestión de incidentes de seguridad de la información. Define procesos para detectar, responder y aprender de incidentes. Muy útil para SOC que manejan respuesta a incidentes.

MITRE ATT&CK Framework
MITRE Corporation.

Evalúa la capacidad del SOC para detectar y responder a técnicas específicas de ataque. Basado en inteligencia real, útil para pruebas de detección y simulaciones. Considera diversas áreas clave como las Técnicas de adversarios, cobertura de detección, mapeo de alertas.

Capability Maturity Model Integration (CMMI) / SOC-CMM.

Evaluación del nivel de madurez de un SOC en múltiples dimensiones (procesos, tecnología, personas). Es una adaptación específica para SOCs que nos permitirá establecer una hoja de ruta de mejora continua desde un nivel inicial (ad hoc) hasta optimizado (mejora continua). Es certificable por terceros.

ENS (Esquema Nacional de Seguridad – España)

Es de obligatorio cumplimiento para entidades públicas y proveedores tecnológicos en España. Se alinea con ISO 27001, incluye requisitos específicos para entornos críticos. Establece distintas categorías de seguridad, medidas organizativas, operativas y de protección. Es certificable por terceros.

ISO 20000

Es un modelo internacional ISO que establece las especificaciones y criterios para la Gestión de servicios TI, incluyendo operaciones de seguridad. Mejora la integración del SOC con el resto de la organización TI. Considera una serie de ámbitos o procesos específicos que regular como la gestión de incidentes, cambios, niveles de servicio, etc. Es certificable por terceros.

No obstante, La Directiva NIS2 (UE 2022/2555), en vigor desde enero de 2023, representa un salto cualitativo con respecto a la auditoría externa de servicios de SOC. Teniendo en cuenta que su objetivo es reforzar la resiliencia digital de los sectores esenciales e importantes, está imponiendo requisitos más estrictos de gestión de riesgos, gobernanza y supervisión. Aunque NIS2 no impone directamente un esquema de certificación obligatorio, sí establece un marco que garantice que las entidades cumplan con medidas técnicas y organizativas adecuadas, y permite a las autoridades competentes de cada país realizar auditorías para verificar el cumplimiento de los requisitos que establece.

En este contexto, los SOCs, como servicios críticos de ciberseguridad, se ven directamente afectados. La necesidad de demostrar su capacidad técnica, fiabilidad operativa y cumplimiento normativo está impulsando el desarrollo de modelos de certificación específicos para servicios gestionados de seguridad.

ENISA, bajo el marco del Cybersecurity Act, está trabajando en la ampliación de esquemas de certificación que incluyan servicios gestionados de ciberseguridad, como los SOC.

En breve podremos disponer de un esquema de certificación que servirá de estándar y que permitirá la evaluación de capacidades, utilidad y gestión de la mejora continua a la que probablemente todos los proveedores que conocemos en nuestro entorno se sumarán.

11.5. INTRODUCCIÓN AL **RED TEAMING**

En la auditoría externa se visibiliza la alineación contra el modelo para todo el público, quedando evidenciado el compromiso mediante la generación de un certificado de cumplimiento y en muchos casos la publicación del certificado para su consulta por parte de terceros. Esta publicación permite evidenciar la alineación de nuestro servicio con un modelo o estándar. En definitiva, se pretende "certificar" el nivel de cumplimiento de nuestro servicio con los requisitos que se establecen en el modelo de referencia. El siguiente listado no excluyente representa los modelos más representativos en la actualidad, en algunos casos serán certificables por terceros y en otros no:

¿Qué es un Red Team?

Un Red Team es un equipo técnico especializado en realizar ataques controlados y autorizados contra los activos de una organización. Su propósito no es causar daño, sino actuar como un adversario realista para poner a prueba los sistemas, procesos y personas responsables de la defensa. Esta práctica se desarrolla bajo condiciones planificadas, acordadas con antelación, y en ocasiones, con conocimiento limitado por parte del resto del personal técnico, para evaluar la respuesta en condiciones reales.

A diferencia de otros ejercicios más acotados como las pruebas de penetración, el Red Teaming no busca simplemente encontrar fallos técnicos, sino evaluar cómo interactúan las distintas capas de seguridad, incluyendo la detección, la respuesta operativa, la comunicación y la toma de decisiones por parte de la organización.

Alcance y metodologías

El alcance de un ejercicio de Red Teaming puede variar según los objetivos definidos previamente. Algunas de las actividades que suelen llevarse a cabo incluyen:

- Ingeniería social para evaluar el nivel de concienciación del personal.
- Simulación de acceso físico a instalaciones con fines de intrusión.
- Acceso remoto a sistemas mediante técnicas como phishing o explotación de vulnerabilidades.
- Movimientos laterales en la red y elevación de privilegios.
- Exfiltración de datos para comprobar los mecanismos de control y alerta.

Estas acciones se diseñan cuidadosamente para evitar impactos negativos y deben ejecutarse dentro de un marco ético y legal claramente establecido.

Los ejercicios suelen basarse en metodologías como las del marco MITRE ATT&CK, que permiten estructurar las campañas ofensivas utilizando técnicas observadas en ciberataques reales.

Valor para la mejora continua del SOC

El Red Teaming ofrece una fuente valiosa de información para retroalimentar el proceso de mejora continua. Al enfrentarse a ataques realistas, el equipo del SOC tiene la oportunidad de validar sus procedimientos en condiciones similares a las de un incidente real. Esta validación incluye la eficacia de los casos de uso configurados en las herramientas de monitoreo, la precisión de las alertas, la velocidad de respuesta y la coordinación entre áreas.

Los hallazgos obtenidos permiten identificar brechas de seguridad, fallos de configuración, debilidades en la formación del personal o limitaciones en la cobertura de herramientas. A partir de esta información, se generan planes de acción que fortalecen la postura defensiva de la organización.

Ejemplo práctico

Una organización planifica un ejercicio de Red Teaming con el objetivo de evaluar su nivel de preparación frente a un ataque dirigido. El equipo atacante simula un correo de phishing dirigido a personal del área financiera. Una persona hace clic en el enlace y permite el acceso remoto a su equipo. El Red Team logra moverse lateralmente por la red interna sin ser detectado durante varias horas. Tras concluir el ejercicio, se identifican deficiencias en las reglas de detección del SIEM y en la supervisión de comportamientos anómalos. Como respuesta, se rediseñan los casos de uso, se actualizan las herramientas de seguridad y se ofrece formación adicional al personal afectado.

Cómo integrar el Red Teaming en la mejora continua

La integración del Red Teaming en el proceso de mejora continua fortalece significativamente la capacidad de una organización para adaptarse a un entorno de amenazas cada vez más sofisticado. Al incorporar de forma sistemática este tipo de ejercicios dentro del ciclo operativo del centro de operaciones de seguridad (Security Operations Center, en adelante, "SOC"), es posible identificar debilidades reales, validar controles y generar una evolución constante en las defensas.

Planificación estratégica del Red Teaming

El primer paso para integrar el Red Teaming en la mejora continua consiste en definir con claridad los objetivos del ejercicio. Estos pueden orientarse a evaluar la detección de un tipo específico de amenaza, comprobar la eficacia de los protocolos de respuesta o validar los mecanismos de comunicación interna durante un incidente.

La planificación debe incluir:

- La definición del alcance: qué sistemas, servicios o procesos se verán involucrados.
- La aprobación del ejercicio por parte de la Dirección.
- El establecimiento de un cronograma y responsables.
- El diseño de escenarios basados en amenazas relevantes para la organización.
- La identificación de indicadores de éxito y criterios de evaluación.

Durante esta etapa, resulta útil recurrir a técnicas de análisis de amenazas como el enfoque de inteligencia de amenazas (Threat Intelligence) y marcos como MITRE ATT&CK, que ayudan a seleccionar tácticas y técnicas realistas empleadas por adversarios reales.

Ejecución de los ejercicios

La ejecución del ejercicio debe desarrollarse de forma controlada, respetando los límites establecidos en la fase de planificación. Es habitual que solo un grupo reducido dentro del SOC tenga conocimiento del inicio y las acciones que se realizarán, con el fin de mantener la naturalidad de la respuesta.

Durante la actividad ofensiva, el equipo atacante simula técnicas como el envío de correos electrónicos fraudulentos (phishing), la explotación de vulnerabilidades técnicas, la evasión de controles de seguridad, el movimiento lateral dentro de la red o la exfiltración de información.

La clave de esta fase no reside únicamente en realizar la intrusión, sino en observar cómo responde el equipo defensivo, qué alertas se generan, cuánto tiempo se tarda en identificar el ataque y qué decisiones se toman.

Documentación de hallazgos

Una vez finalizado el ejercicio, el Red Team debe elaborar un informe detallado en el que se incluyan:

- Las técnicas utilizadas.
- Las acciones realizadas y los sistemas comprometidos.
- Los puntos donde la organización detectó o no la actividad maliciosa.
- Las debilidades identificadas en procesos, herramientas o formación.
- Recomendaciones de mejora para cada hallazgo

Este informe se convierte en un input clave para la fase de análisis del ciclo de mejora continua, permitiendo a las diferentes áreas revisar sus procedimientos y establecer planes de acción concretos.

Aplicación de medidas correctivas

A partir de los hallazgos, la organización debe implementar medidas que fortalezcan sus capacidades. Estas pueden incluir:

- La reconfiguración de herramientas de seguridad, como el sistema de información y gestión de eventos (SIEM).
- La creación o ajuste de reglas de detección y casos de uso.
- La formación del personal técnico en las técnicas utilizadas durante el ejercicio.
- La revisión de procesos de respuesta y de escalado de incidentes.
- La incorporación de nuevos controles tecnológicos o manuales.

Cada una de estas acciones debe formar parte de un plan de mejora documentado, con responsables, plazos y mecanismos de seguimiento. Así, el conocimiento generado por el Red Teaming no se limita a un ejercicio puntual, sino que se transforma en un cambio real y sostenible.

Ejemplo práctico

Una organización incluye, dentro de su estrategia anual de seguridad, la realización de un ejercicio de Red Teaming orientado a simular una amenaza interna. El equipo atacante logra acceder a una base de datos sensible desde una cuenta comprometida. El análisis posterior revela que el monitoreo de actividades internas carece de correlación entre el comportamiento del usuario y los datos accedidos. Como parte de las acciones de mejora, se implementan nuevas reglas en el SIEM, se refuerzan los controles de acceso y se establece un sistema de alertas basado en análisis de comportamiento.

11.6. INTRODUCCIÓN AL **PURPLE TEAMING**

El concepto de Purple Teaming surge como respuesta a la necesidad de colaboración entre los equipos ofensivos y defensivos dentro de una organización. Este enfoque permite mejorar de forma coordinada las capacidades de detección, análisis y respuesta ante amenazas reales, mediante ejercicios prácticos que simulan el comportamiento de actores maliciosos.

¿Qué es Purple Teaming?

El término Purple Team combina los enfoques del Red Team (responsable de simular ataques) y el Blue Team (encargado de la defensa). A diferencia de un ejercicio tradicional de tipo ofensivo, donde el equipo defensor desconoce las acciones realizadas por el adversario, el enfoque Purple promueve la cooperación directa entre ambos grupos. Esta colaboración tiene como objetivo validar y mejorar los controles existentes, fortalecer los mecanismos de respuesta y optimizar el monitoreo continuo de amenazas.

A través del Purple Teaming, se busca establecer una dinámica de aprendizaje conjunto: mientras un grupo ejecuta técnicas de ataque, el otro analiza la visibilidad del entorno, ajusta sus herramientas y responde en tiempo real. Esta interacción permite identificar brechas en la cobertura de seguridad y aplicar correcciones de manera inmediata.

Beneficios de aplicar este enfoque en el SOC

El Purple Teaming representa una herramienta muy valiosa dentro del proceso de mejora continua, ya que permite:

- Validar la eficacia de los casos de uso implementados en sistemas de información y gestión de eventos de seguridad (SIEM).
- Ajustar las reglas de correlación y detección para responder ante técnicas reales de ataque.
- Evaluar la capacidad del equipo de seguridad para interpretar indicadores de compromiso (Indicators of Compromise, IOC).
- Identificar puntos ciegos en la infraestructura tecnológica, como la falta de registros en sistemas críticos o deficiencias en la recolección de datos.
- Fomentar una cultura colaborativa entre áreas tradicionalmente separadas.

Este enfoque también mejora la comunicación técnica y táctica entre las personas responsables de diseñar la defensa y quienes la ponen a prueba. Como resultado, la organización adquiere una visión más integral de sus capacidades reales frente a amenazas externas.

Relación con marcos de referencia

La metodología Purple Team se puede estructurar en torno a marcos reconocidos como la matriz MITRE ATT&CK. Esta matriz ofrece una clasificación detallada de tácticas, técnicas y procedimientos (TTP) utilizados por atacantes reales. Al utilizarla como referencia, las organizaciones pueden planificar ejercicios Purple que simulen técnicas específicas y comprobar si sus herramientas detectan las actividades asociadas.

El marco MITRE ATT&CK permite establecer una línea base de cobertura defensiva, identificar técnicas sin monitoreo adecuado y priorizar ajustes según el nivel de riesgo. Esto convierte al Purple Teaming en una práctica clave para alinear las capacidades del SOC con estándares internacionales.

Ejemplo práctico

Durante un ejercicio de Purple Teaming, un grupo técnico simula un movimiento lateral en la red interna mediante una herramienta legítima de administración remota. Mientras se ejecuta esta acción, el equipo de defensa analiza si existen alertas configuradas que puedan detectar ese comportamiento. Al observar que el evento no genera ningún aviso, se concluye que hay una laguna en los controles de seguridad. A partir de este hallazgo, se actualizan las reglas del SIEM y se incorporan nuevas fuentes de registro para incrementar la visibilidad. En futuras pruebas, la actividad es identificada y contenida en menos de cinco minutos.

Cómo implementar el Purple Teaming en el ciclo de mejora

El Purple Teaming se consolida como una estrategia clave para optimizar las defensas de una organización de forma progresiva, colaborativa y medible. Al integrarse dentro del ciclo de mejora continua, esta práctica permite comprobar en tiempo real la eficacia de los controles, reducir la brecha entre los equipos ofensivos y defensivos, y promover una cultura técnica orientada al aprendizaje constante.

Enfoque colaborativo para la mejora

A diferencia de los ejercicios de Red Teaming, que suelen ejecutarse sin el conocimiento del equipo defensor, el Purple Teaming se basa en la cooperación entre quienes simulan ataques y quienes se encargan de la defensa. Esta colaboración permite que cada técnica ofensiva sea inmediatamente analizada, detectada, y corregida si no se encuentra cubierta adecuadamente.

Este enfoque rompe con la visión tradicional de competencia entre equipos y la reemplaza por una dinámica orientada a la mejora del conjunto. En esta dinámica, cada ataque se convierte en una oportunidad para identificar deficiencias, ajustar las herramientas y reforzar los procedimientos de respuesta.

Integración con el ciclo de mejora continua

Esta integración se realiza a través de las siguientes fases:

a) Planificación del ejercicio

La organización define los objetivos específicos del ejercicio, que pueden estar enfocados en probar un conjunto de controles, validar nuevos casos de uso o explorar una categoría particular de técnicas ofensivas. Se seleccionan los participantes y se establecen los indicadores de éxito que se utilizarán para evaluar los resultados.

Para estructurar el contenido del ejercicio, se suele emplear la matriz MITRE ATT&CK, que permite seleccionar técnicas representativas de amenazas reales. También se pueden incorporar escenarios basados en análisis de amenazas propias de la organización o del sector al que pertenece.

b) Ejecución coordinada

Durante la ejecución, el equipo ofensivo simula un ataque mientras el equipo defensivo observa y analiza su respuesta. Esta interacción permite validar alertas, mejorar la visibilidad de los eventos y optimizar la lógica de detección en herramientas como el sistema de información y gestión de eventos (SIEM), soluciones de detección y respuesta en endpoints (EDR) o firewalls de nueva generación.

Cada técnica se prueba, se observa su efecto, y se ajustan las configuraciones de seguridad en tiempo real o en ejercicios posteriores, dependiendo del tipo de entorno y nivel de riesgo aceptado.

c) Registro y análisis de resultados

El proceso de Purple Teaming requiere un seguimiento detallado de cada fase. Es recomendable documentar cada técnica utilizada, los controles activados, las deficiencias observadas y las acciones tomadas para subsanar errores. Este registro permite retroalimentar el ciclo de mejora continua con datos precisos y accionables.

d) Aplicación de mejoras

Los hallazgos del ejercicio se transforman en ajustes concretos, como:

- Nuevas reglas de correlación.
- Ampliación de fuentes de registro.
- Ajustes de configuración en herramientas de monitoreo.
- Modificaciones en procesos de respuesta.
- Capacitación dirigida a los equipos técnicos.

Además, se pueden desarrollar automatizaciones en plataformas de orquestación y respuesta ante incidentes (SOAR) para reducir los tiempos de reacción ante eventos similares en el futuro[1].

Ventajas del Purple Teaming en entornos operativos

La implementación de esta práctica ofrece ventajas claras para las organizaciones:

- Mejora continua basada en pruebas reales y medibles.
- Reducción de puntos ciegos en la infraestructura tecnológica.
- Fomento de la comunicación entre equipos técnicos.
- Mayor velocidad de detección y respuesta.
- Priorización de mejoras en función del riesgo.

Este enfoque resulta especialmente útil en entornos donde el SOC está en etapa de madurez intermedia, ya que permite evolucionar de una operación centrada en eventos reactivos hacia una postura proactiva y dinámica.

Ejemplo práctico

Una organización incorpora ejercicios de Purple Teaming como parte de sus actividades mensuales. En un ejercicio reciente, se simula el uso de una herramienta legítima para ejecutar comandos de administración en un servidor interno. El equipo defensor no recibe ninguna alerta, lo que revela una ausencia de monitoreo sobre ciertos procesos de sistema. Como resultado, se actualizan las fuentes de registro, se crean nuevas reglas de correlación en el SIEM y se capacita al personal sobre técnicas de **living off the land**[2] (uso de herramientas del propio entorno para ejecutar acciones maliciosas). Al repetir la prueba semanas después, la actividad es detectada de inmediato y contenida eficazmente.

[1]SOAR (Security Orchestration, Automation and Response): plataforma que permite automatizar tareas de seguridad, coordinar herramientas y gestionar la respuesta ante incidentes de forma estructurada. Referencia: Centro de Ciberseguridad Industrial (CCI).

[2]Living off the land: técnica en la que una persona atacante utiliza herramientas y funcionalidades legítimas del entorno para evitar la detección. Referencia: MITRE ATT&CK.

11.7. CASOS DE USO **PRÁCTICOS**

Estos ejercicios permiten identificar fallos en tiempo real, ajustar configuraciones críticas, desarrollar capacidades del personal y, sobre todo, convertir la experiencia en conocimiento útil para la organización.

A través de casos de uso prácticos, es posible comprender de forma más clara cómo se implementan y aprovechan estos ejercicios dentro del ciclo de mejora continua. Los siguientes ejemplos han sido elaborados de manera ficticia para ilustrar escenarios comunes en organizaciones de diversos sectores.

Caso 1: Optimización de reglas de detección tras ejercicio de Purple Teaming

Contexto:

Una organización del sector educativo realiza un ejercicio de Purple Teaming centrado en simular técnicas de acceso inicial y ejecución remota de comandos. Se emplean comandos de PowerShell para establecer una comunicación inversa con un servidor controlado por el equipo atacante.

Hallazgo:

El sistema de información y gestión de eventos (SIEM) no cuenta con reglas específicas para detectar la combinación de eventos generados por esta actividad. Además, algunos registros clave de ejecución no están habilitados en los endpoints del personal docente.

Mejoras implementadas:

Se activan políticas de auditoría en los sistemas afectados.

Se incorporan nuevas fuentes de registro.

Se crea una regla de correlación en el SIEM que relaciona el uso de PowerShell con conexiones salientes inusuales.

El personal del SOC recibe formación específica sobre técnicas de evasión utilizando herramientas del sistema.

`Resultado:`

Al repetir la prueba semanas después, el evento genera una alerta automática que es gestionada en menos de cinco minutos.

Caso 2: Fortalecimiento del plan de respuesta ante incidentes tras campaña de Red Teaming

Contexto:

Durante un ejercicio de Red Teaming, una organización simula un escenario donde una persona atacante logra obtener credenciales administrativas mediante un ataque de phishing. A partir de allí, el atacante accede al sistema de correo interno y realiza movimientos laterales hacia otros servidores.

Hallazgo:

El SOC no dispone de un procedimiento específico para gestionar accesos internos anómalos desde cuentas privilegiadas. La respuesta se retrasa y se identifica una falta de coordinación entre el equipo técnico y la Dirección de Tecnología.

Mejoras implementadas:

Se actualiza el plan de respuesta ante incidentes, incorporando protocolos específicos para compromisos internos.

Se automatiza la desactivación temporal de cuentas privilegiadas en caso de actividades inusuales.

Se asignan responsables por área para mejorar los tiempos de escalado.

Se realiza un simulacro con todos los equipos involucrados en la gestión de incidentes.

`Resultado:`

En una simulación posterior, un evento similar es contenido en menos de 30 minutos, gracias a la actuación conjunta del equipo técnico y la Dirección de Tecnología.

Caso 3: Mejora de la visibilidad en sistemas críticos

Contexto:

En una organización del sector salud, se ejecuta una campaña de Purple Teaming enfocada en técnicas de persistencia mediante modificaciones del registro de Windows. El ejercicio demuestra que la actividad no es detectada, debido a la falta de registros provenientes de los sistemas clínicos.

Hallazgo:

El SOC no recibe datos relevantes de los sistemas hospitalarios críticos, lo que genera puntos ciegos. Tampoco existen reglas específicas para identificar cambios en configuraciones clave.

Mejoras implementadas:

Se integran los sistemas hospitalarios al SIEM mediante conectores compatibles.

Se diseñan reglas que monitorean cambios en claves del registro vinculadas a persistencia.

Se definen perfiles de comportamiento esperado en estos entornos.

Se refuerza la capacitación del personal clínico para reportar actividades inusuales.

Resultado:

La cobertura del SOC se amplía y se detectan intentos de modificación no autorizados durante una auditoría posterior.

Conclusión

Estos casos ilustran cómo los ejercicios de Red Teaming y Purple Teaming ofrecen una vía directa para transformar las debilidades en oportunidades de fortalecimiento. Su integración en el ciclo de mejora continua permite a la organización no solo detectar vulnerabilidades, sino también construir una defensa más adaptativa, precisa y centrada en sus activos más críticos.

11.8. **MÉTRICAS Y KPIs** PARA EVALUAR LA MEJORA CONTINUA

Las métricas y los indicadores clave de rendimiento (Key Performance Indicators, en adelante, "KPI") permiten a la organización medir de forma sistemática la eficacia de sus procesos, identificar áreas de mejora y demostrar avances concretos en materia de ciberseguridad.

Importancia de medir el desempeño

Contar con métricas claras facilita la toma de decisiones basada en datos. Estos indicadores permiten a la Dirección de Tecnología y al equipo del SOC analizar si las acciones emprendidas generan los resultados esperados, y si es necesario ajustar herramientas, procedimientos o asignaciones de recursos. Además, favorecen la transparencia interna, la rendición de cuentas y el alineamiento con los objetivos estratégicos de la organización.

En el contexto del Red Teaming y Purple Teaming, las métricas permiten identificar la evolución del nivel de madurez defensiva, la capacidad de detección ante técnicas específicas, y el impacto real de las mejoras implementadas tras cada ejercicio.

Principales KPIs para un SOC orientado a la mejora continua

A continuación, se describen algunos indicadores clave ampliamente utilizados en entornos operativos de seguridad:

a) Tiempo medio de detección (MTTD)

Este KPI mide el promedio de tiempo que transcurre entre el inicio de una actividad maliciosa y su detección por parte del SOC. Un valor elevado puede indicar deficiencias en la cobertura de alertas, en el monitoreo o en la visibilidad de registros.

Ejemplo: si durante un ejercicio de Red Teaming se detecta una actividad 24 horas después de su ejecución, se considera que el MTTD requiere ser optimizado mediante nuevos casos de uso o mejoras en el SIEM.

b) Tiempo medio de respuesta (MTTR)

Representa el promedio de tiempo que transcurre entre la detección de un incidente y su contención o resolución. Este indicador refleja la agilidad del equipo ante eventos reales o simulados.

Ejemplo: tras un ejercicio de Purple Teaming, se mide el tiempo que tarda el equipo en responder a una simulación de exfiltración de datos. Si el MTTR supera los 60 minutos, se evalúa la automatización de tareas repetitivas mediante soluciones SOAR[1].

c) Porcentaje de técnicas detectadas (cobertura ATT&CK)

Este KPI mide qué proporción de las técnicas utilizadas durante un ejercicio (basadas en la matriz MITRE ATT&CK) son detectadas de forma efectiva por los sistemas defensivos. Permite visualizar la cobertura técnica del SOC frente a amenazas reales.

Ejemplo: si en un ejercicio se emplean diez técnicas diferentes y solo se detectan cinco, el nivel de cobertura es del 50 % y se establece como prioridad ampliar la visibilidad sobre las restantes.

d) Número de acciones de mejora implementadas

Este indicador permite medir el volumen de mejoras aplicadas tras ejercicios de simulación o incidentes reales. Incluye cambios en herramientas, ajustes de configuración, actualizaciones de procedimientos y formación del personal.

Ejemplo: un informe post ejercicio de Red Teaming identifica seis mejoras, de las cuales cuatro son implementadas en un plazo de dos semanas.

e) Reducción del número de falsos positivos

Un alto número de alertas sin relevancia puede saturar al personal del SOC y retrasar la respuesta ante amenazas reales. Este KPI evalúa la calidad de las reglas de detección y la precisión de los controles automatizados.

Ejemplo: luego de realizar ajustes basados en Purple Teaming, se observa una reducción del 30 % en el volumen de alertas innecesarias, mejorando la eficiencia operativa.

[1]SOAR (Security Orchestration, Automation and Response): solución tecnológica que permite automatizar tareas de seguridad, mejorar la gestión de alertas y coordinar la respuesta a incidentes. Referencia: Centro de Ciberseguridad Industrial (CCI).

Recomendaciones para la implementación de métricas

Para que las métricas sean útiles, es necesario que cumplan con ciertas características:

- **Relevancia: deben estar alineadas con los objetivos de seguridad de la organización.**
- **Claridad: deben ser comprensibles por todos los perfiles del equipo técnico.**
- **Comparabilidad: deben poder medirse de forma periódica y consistente.**
- **Accionabilidad: deben permitir tomar decisiones concretas a partir de sus resultados.**

Además, se recomienda utilizar herramientas de visualización como paneles de control o informes automatizados que faciliten el seguimiento de estos KPIs a lo largo del tiempo.

Ejemplo práctico

Una organización realiza ejercicios trimestrales de Purple Teaming. En cada ejercicio, se registran el tiempo medio de detección, el porcentaje de técnicas detectadas y las acciones de mejora derivadas. A lo largo de un año, el MTTD se reduce de cuatro horas a 30 minutos, y la cobertura ATT&CK se incrementa del 40 % al 85 %. Estos resultados permiten justificar la inversión en nuevas herramientas y demuestran la efectividad del enfoque colaborativo en la mejora continua.

11.9. **HERRAMIENTAS** DE APOYO

La mejora continua en un SOC no puede depender únicamente del esfuerzo humano. La disponibilidad de herramientas adecuadas es clave para facilitar la detección de amenazas, automatizar procesos, reducir errores y acelerar los ciclos de aprendizaje. Estas soluciones tecnológicas permiten implementar ejercicios de Red Teaming y Purple Teaming de forma estructurada, medible y eficiente.

Contar con un conjunto de herramientas bien integradas no solo mejora la capacidad de respuesta ante incidentes, sino que también fortalece el ciclo de mejora continua, al proporcionar evidencia técnica, indicadores y datos procesables para aplicar cambios concretos en la defensa.

Tipologías de herramientas utilizadas en el SOC

A continuación, se describen los tipos de herramientas más utilizadas en actividades relacionadas con Red Teaming, Purple Teaming y mejora continua:

a) Herramientas de simulación de ataque

Estas soluciones permiten ejecutar técnicas ofensivas de forma controlada y automatizada, basadas en comportamientos observados en ataques reales. Están diseñadas para simular tácticas y procedimientos usados por grupos maliciosos, facilitando la validación de controles defensivos.

Ejemplos destacados:

- **Atomic Red Team:** biblioteca de pruebas desarrollada por Red Canary que permite simular técnicas específicas del marco MITRE ATT&CK. Es de código abierto y ampliamente utilizada por SOCs en procesos de validación de detección9.
- **CALDERA:** plataforma automatizada del MITRE diseñada para ejecutar operaciones de Red Teaming y Purple Teaming utilizando agentes que interactúan con sistemas simulados o reales.
- **SimuLand:** entorno de laboratorio desarrollado por Microsoft que permite probar técnicas ofensivas en infraestructuras controladas de Microsoft 365 y Azure.

Estas herramientas permiten realizar pruebas sin causar interrupciones en la operación y están diseñadas para facilitar la retroalimentación inmediata.

b) Herramientas de monitoreo, detección y análisis

Son las soluciones encargadas de recolectar eventos, analizarlos y generar alertas ante comportamientos sospechosos. Estas herramientas constituyen el núcleo de la actividad del SOC.

Principales tipos:

- **SIEM** (Security Information and Event Management)
- **EDR** (Endpoint Detection and Response)
- **NDR** (Network Detection and Response)

La integración de estas herramientas con plataformas de simulación permite validar la capacidad de detección de amenazas reales.

c) Plataformas de orquestación y automatización (SOAR)

Estas herramientas permiten coordinar múltiples sistemas de seguridad, automatizar respuestas y gestionar flujos de trabajo ante incidentes. Reducen el tiempo de respuesta y mejoran la eficiencia del equipo técnico.

Funcionalidades destacadas:

- Automatización de tareas repetitivas, como el cierre de sesiones sospechosas o el aislamiento de dispositivos.
- Generación automática de tickets y alertas.
- Integración con herramientas de simulación y análisis para facilitar la mejora continua.

d) Repositorios y bases de conocimiento

El uso de marcos estructurados y fuentes de información pública ayuda a guiar las acciones del SOC y los ejercicios ofensivos.

Ejemplos comunes:

- **MITRE ATT&CK:** matriz que clasifica técnicas ofensivas utilizadas por actores maliciosos. Sirve como referencia para diseñar casos de uso y validar controles de seguridad.
- **CAPEC** (Common Attack Pattern Enumeration and Classification): base de datos de patrones de ataque que ayuda a comprender el modo de operación de una amenaza.
- **Open Threat Exchange (OTX):** comunidad abierta para compartir indicadores de compromiso y técnicas emergentes.

Consideraciones para su implementación

La selección de herramientas debe adaptarse al tamaño, recursos y necesidades específicas de cada organización. En algunos casos, puede optarse por soluciones de código abierto que ofrecen flexibilidad y bajo coste, mientras que en entornos más exigentes puede requerirse la adquisición de herramientas comerciales con funcionalidades avanzadas.

También es importante considerar:

- La compatibilidad entre las distintas soluciones.
- La facilidad de integración con los sistemas existentes.
- La posibilidad de escalar el uso de la herramienta a medida que el SOC madura.
- El soporte y la comunidad que respaldan su uso.

Ejemplo práctico

Una organización de tamaño medio implementa Atomic Red Team para simular ataques basados en técnicas de movimiento lateral. Estas simulaciones se conectan con el SIEM, que genera alertas configuradas previamente. Sin embargo, algunas técnicas no son detectadas. A partir de este ejercicio, se ajustan las reglas del SIEM, se amplía la recopilación de registros y se automatiza la respuesta mediante una solución SOAR. El resultado es una mejora concreta en la detección y tiempos de respuesta.

Atomic Red Team: conjunto de pruebas de seguridad diseñado para simular técnicas ofensivas específicas. Recurso de código abierto desarrollado por Red Canary.

SOAR (Security Orchestration, Automation and Response): tecnología que permite automatizar tareas, coordinar herramientas de seguridad y gestionar la respuesta a incidentes. Referencia: Centro de Ciberseguridad Industrial (CCI).

11.10. DESAFÍOS COMUNES Y RECOMENDACIONES

La implementación de una estrategia de mejora continua en un SOC que incluya ejercicios de Red Teaming y Purple Teaming, presenta numerosos beneficios. Sin embargo, también implica enfrentar ciertos desafíos técnicos, organizativos y culturales que pueden dificultar su adopción o limitar su efectividad.

Reconocer estas dificultades permite a la organización anticiparse y diseñar soluciones adecuadas para que las iniciativas de mejora continua se sostengan en el tiempo y generen un impacto real en la seguridad.

Principales desafíos en la implementación

a) Falta de cultura colaborativa entre equipos

Uno de los obstáculos más frecuentes es la separación tradicional entre equipos ofensivos (que prueban la seguridad) y defensivos (que la operan). Esta división puede generar conflictos de intereses, falta de comunicación o incluso desconfianza, dificultando los ejercicios de Purple Teaming, que dependen de una colaboración fluida.

Situación común: El equipo técnico ve al Red Team como una figura crítica en lugar de una aliada para el aprendizaje, lo que limita el aprovechamiento de los ejercicios.

b) Recursos limitados

Muchas organizaciones, especialmente de tamaño pequeño o mediano, cuentan con presupuestos y personal reducidos para funciones de ciberseguridad. Esto puede limitar la frecuencia de los ejercicios, el uso de herramientas avanzadas o la dedicación de personas para análisis y seguimiento.

Situación común: El SOC dispone de un número reducido de analistas que deben cubrir múltiples funciones, lo que dificulta dedicar tiempo a la revisión posterior de cada ejercicio o a la implementación de mejoras.

c) Escasa formación especializada

El diseño, ejecución y aprovechamiento de ejercicios ofensivos requiere habilidades técnicas específicas, tanto en técnicas de ataque como en análisis de resultados. Cuando no se cuenta con personal formado en estas áreas, los ejercicios pueden volverse poco realistas o difíciles de interpretar.

Situación común: Los equipos realizan simulaciones limitadas a técnicas básicas, sin capacidad para ajustar configuraciones ni entender completamente los hallazgos.

d) Dificultad para medir resultados

La mejora continua exige indicadores y datos que permitan evaluar el avance real del SOC. En ocasiones, las organizaciones no cuentan con métricas adecuadas o los datos disponibles no están organizados de forma que puedan utilizarse para guiar decisiones.

Situación común: Se realizan ejercicios periódicos, pero no se comparan sus resultados ni se documenta la evolución de la cobertura de detección, lo que impide conocer si las capacidades del SOC han mejorado.

Recomendaciones para superar los desafíos

1. Fomentar una cultura de cooperación

Es fundamental promover la colaboración entre las diferentes áreas técnicas. Para ello, se recomienda:

- Establecer objetivos comunes entre el equipo ofensivo y defensivo.
- Reforzar la visión de que el aprendizaje es compartido y no punitivo.
- Incorporar al Purple Teaming como práctica regular, con participación activa del personal.

2. Empezar con ejercicios de bajo coste y alta efectividad

La mejora continua no requiere grandes inversiones iniciales. Las organizaciones pueden comenzar con simulaciones sencillas utilizando herramientas de código abierto como Atomic Red Team o CALDERA. Estas permiten realizar pruebas reales con una inversión mínima, y obtener resultados útiles para ajustar configuraciones y procedimientos.

3. Capacitar progresivamente al equipo

El desarrollo de competencias técnicas es un proceso gradual. La organización puede:

- Incorporar módulos de formación en técnicas ofensivas y defensivas.
- Fomentar la participación en comunidades abiertas de ciberseguridad.
- Utilizar entornos de laboratorio o simuladores para practicar sin riesgos.

4. Definir y mantener un sistema de métricas

Para medir el impacto real de las actividades de mejora, se recomienda definir un conjunto reducido de indicadores clave (KPIs) y mantener un registro histórico. Esto permite visualizar la evolución del SOC y justificar decisiones estratégicas.

5. Documentar y socializar los aprendizajes

Cada ejercicio o incidente ofrece lecciones valiosas. Para consolidarlas, se sugiere:

- Elaborar informes accesibles para distintos niveles de la organización.
- Compartir hallazgos relevantes con otras áreas (por ejemplo, sistemas, desarrollo, cumplimiento).
- Incorporar los aprendizajes en sesiones de formación internas.

Ejemplo práctico

Una organización del sector logístico, con recursos limitados, decide realizar ejercicios de Purple Teaming trimestrales utilizando herramientas abiertas. Durante el primer año, los ejercicios son simples y se centran en técnicas básicas de reconocimiento y movimiento lateral. A lo largo del tiempo, se documentan más de veinte ajustes implementados en el SIEM, y el tiempo medio de detección disminuye de tres horas a cuarenta y cinco minutos. La Dirección de Tecnología reconoce el avance, y se decide ampliar la cobertura del SOC con personal especializado.

11.11. CONCLUSIÓN

La mejora continua es una condición indispensable para que cualquier organización pueda mantener un SOC eficiente, resiliente y alineado con la evolución constante de las amenazas digitales. En un entorno cambiante, donde las técnicas utilizadas por actores maliciosos se sofistican día a día, solo aquellas organizaciones que adoptan un enfoque sistemático de evaluación, corrección y aprendizaje podrán garantizar una defensa sostenida en el tiempo.

El presente bloque ha demostrado que la integración de ejercicios de Red Teaming y Purple Teaming dentro del ciclo de mejora continua permite a la organización:

- Evaluar su capacidad real de detección y respuesta ante técnicas ofensivas utilizadas en incidentes reales.
- Validar y ajustar controles de seguridad, reglas de correlación y fuentes de registro.
- Fortalecer los procedimientos de respuesta ante incidentes mediante la observación de escenarios controlados.
- Reducir los tiempos medios de detección y contención de amenazas.
- Aumentar la cobertura sobre técnicas documentadas en marcos reconocidos como MITRE ATT&CK.

El enfoque colaborativo promovido por el Purple Teaming, en particular, ha mostrado ser un catalizador clave para la madurez del SOC, ya que impulsa la cooperación entre los equipos ofensivos y defensivos, fomenta una cultura orientada al aprendizaje y acelera la evolución de la postura defensiva. Este tipo de práctica, accesible incluso para organizaciones con recursos limitados, ofrece resultados concretos en la optimización de la operación diaria.

A su vez, la planificación periódica de ejercicios de Red Teaming, con objetivos claramente definidos y análisis estructurado de resultados, permite identificar debilidades que de otro modo podrían pasar inadvertidas hasta que se materialice una amenaza. Estos ejercicios sirven como simulaciones realistas de ataques dirigidos, que ponen a prueba no solo las capacidades técnicas, sino también la coordinación, la comunicación y la toma de decisiones ante crisis.

La implementación exitosa de esta estrategia requiere, sin embargo, del acompañamiento de métricas, herramientas adecuadas, formación continua y un entorno que valore el aprendizaje por encima del error. Las organizaciones que logran alinear estos elementos se posicionan con una ventaja significativa frente a los riesgos actuales y emergentes.

Reflexión final

Más allá de la tecnología, la mejora continua en ciberseguridad es una cuestión de actitud organizacional. Es el compromiso de revisar lo que se hace, entender por qué se hace y buscar siempre cómo hacerlo mejor. En este proceso, el Red Teaming y el Purple Teaming no son fines en sí mismos, sino herramientas poderosas para transformar la seguridad de un concepto estático a un proceso vivo, dinámico y en constante evolución.

CONCLUSIONES

12.

En el contexto actual de ciberseguridad, el SOC se ha transformado de una función meramente reactiva a un componente estratégico, dinámico y multifuncional, capaz de anticipar, detectar, responder y recuperar el servicio frente a una amplia gama de amenazas. A lo largo de este libro blanco, hemos recorrido los principales ejes de su evolución, los desafíos a los que se enfrenta, las demandas cambiantes de las organizaciones, los resultados alcanzados y los horizontes futuros que marcarán la próxima generación de SOC.

Evolución del SOC: de lo táctico a lo estratégico

El SOC ha transitado desde equipos aislados centrados exclusivamente en monitoreo de alertas hacia arquitecturas modernas con capacidades avanzadas de inteligencia de amenazas, automatización y orquestación (SOAR) y análisis basado en comportamiento (UEBA). Esta evolución ha sido impulsada por:

- La creciente complejidad del entorno tecnológico (cloud, IoT, redes híbridas).
- El incremento exponencial en el volumen y sofisticación de alertas y ciberataques.
- La necesidad de una visión holística y continua de la postura de seguridad.

Hoy, un SOC moderno es un habilitador de negocio, alineado con la gestión del riesgo organizacional y los objetivos estratégicos que son el principal objetivo del CISO.

Retos persistentes y emergentes

A pesar de los avances, los SOC enfrentan múltiples retos que limitan su eficiencia y efectividad:

- Crecimiento sostenido de alertas y escasez de analistas capacitados o motivados.
- Falsos positivos y la dificultad para priorizar incidentes en base en impacto real.
- Integración deficiente entre distintas herramientas de diferentes fabricantes.
- Retención de talento en un mercado altamente competitivo. Su formación técnica y humana.
- Necesidad de adaptar el SOC a entornos más regulados y distribuidos (multicloud, OT, entornos remotos).

Abordar estos desafíos requiere no solo inversión en tecnología, sino una redefinición de procesos, estructuras de trabajo y modelos operativos.

Necesidades clave de las organizaciones

Las organizaciones modernas demandan un SOC que no solo reaccione, sino que anticipe. Las necesidades más críticas incluyen:

- Visibilidad integral en tiempo real, incluyendo el descubrimiento de los activos a proteger.
- Detección proactiva mediante inteligencia contextualizada.
- Respuesta automatizada que reduzca el tiempo medio de contención.
- Capacidades de Threat Hunting y análisis forense.
- Modelos de operación híbrida o tercerizada (MSSP, MDR) con SLA claros.
- Cumplimiento normativo con trazabilidad auditable de los eventos.
- Colaboración con el resto de funciones de la función de Ciberseguridad (gobernanza, formación,riesgos, red team, etc).
- Soberanía digital.

El SOC debe ser, en definitiva, un aliado del negocio, adaptado a sus procesos y ciclos de decisión.

Resultados (Outcomes) generados por un SOC efectivo

Un SOC bien diseñado y maduro entrega resultados tangibles que impactan directamente en la resiliencia cibernética de la organización:

- Reducción significativa del tiempo de detección y respuesta (MTTD / MTTR).
- Mejora continua de la postura de seguridad y políticas a partir de los aprendizajes de la operación.
- Fortalecimiento de la inteligencia de amenazas interna.
- Mayor confianza en entornos auditados o regulados (como ISO 27001, PCI-DSS, NIST, etc.).
- Contribución directa a la mitigación de riesgos de negocio y resiliencia operativa.
- Disminución clara del número de incidentes y de su impacto en la continuidad del negocio.

Estos beneficios deben ser medibles y la alta dirección los espera como parte del valor entregado por el área de Ciberseguridad.

El futuro del SOC: hacia un modelo autónomo, predictivo y centrado en riesgos

El SOC del futuro no será simplemente más rápido, sino más inteligente, autónomo y predictivo. Algunas tendencias clave que marcarán esta transformación incluyen:

- Adopción de IA generativa para análisis, automatización y resolución avanzada.
- SOC virtuales, híbridos o distribuidos en configuraciones multi-tenant y multi-cloud.
- Integración con modelos de ciberriesgo cuantitativo y modelos de incertidumbre.
- Enfoque en la resiliencia cibernética, no solo en la protección.
- Operación basada en inteligencia, con ciclos iterativos de mejora (técnicas, tácticas y procedimientos basadas en inteligencia de amenazas de ciberseguridad (CTI), MITRE ATT&CK o defensa basada en amenazas).

La evolución también pasa por nuevas métricas de éxito, donde se mide el impacto evitado y la capacidad de adaptación más allá del volumen de alertas gestionadas.

13. REFERENCIAS

Parlamento Europeo y Consejo. (2016). Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Parlamento Europeo y Consejo. (2024). Reglamento (UE) 2024/1689, por el que se establece una normativa armonizada en materia de inteligencia artificial (AI Act). Diario Oficial de la Unión Europea. *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689*

Parlamento Europeo y Consejo. (2022). Directiva (UE) 2022/2555 (NIS2), sobre medidas para un elevado nivel común de ciberseguridad en toda la Unión. Diario Oficial de la Unión Europea. *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=-CELEX%3A32022L2555*

España. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Boletín Oficial del Estado. *https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673*

España. (2021). Ley 11/2021, de medidas de prevención y lucha contra el fraude fiscal. Boletín Oficial del Estado. *https://www.boe.es/buscar/act.php?id=-BOE-A-2021-12842*

España. (2022). Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS). Boletín Oficial del Estado. *https://www.boe.es/buscar/act.php?id=BOE-A-2022-5075*

España. (1996). Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. Boletín Oficial del Estado *https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930*

España. (2017). Ley 9/2017, de Contratos del Sector Público. Boletín Oficial del Estado. *https://www.boe.es/buscar/act.php?id=BOE-A-2017-12902*

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *https://www.iso.org/standard/27001*

Centro Criptológico Nacional (CCN-CERT). (s.f.). Guías técnicas del Esquema Nacional de Seguridad (ENS). *https://www.ccn-cert.cni.es*

Agencia Española de Protección de Datos (AEPD). (s.f.). Guía del RGPD para responsables del tratamiento. *https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf*

Agencia Española de Protección de Datos (AEPD). (s.f.). Guía sobre gestión de brechas de seguridad. *https://www.aepd.es/guias/guia-brechas-seguridad.pdf*

Agencia Española de Protección de Datos (AEPD). (s.f.). Guía sobre uso de algoritmos en la toma de decisiones automatizadas. *https://www.aepd.es*

Agencia Española de Protección de Datos (AEPD). (s.f.). Guía sobre proveedores y encargados del tratamiento. *https://www.aepd.es*

ISMS Forum. (s.f.). Documentación y posicionamientos sobre cumplimiento y ciberseguridad. *https://www.ismsforum.es*

European Union Agency for Cybersecurity (ENISA). (s.f.). Recursos sobre SOC, respuesta a incidentes y notificación. *https://www.enisa.europa.eu*

Centro Criptológico Nacional (CCN-CERT). (s.f.). Recomendaciones sobre SOC, planes de contingencia y auditoría. *https://www.ccn-cert.cni.es*

Agencia Española de Protección de Datos (AEPD) & Commission Nationale de l'Informatique et des Libertés (CNIL). (s.f.). Documentos sobre transparencia algorítmica, decisiones automatizadas y tratamientos de riesgo. *https://www.aepd.es* y *https://www.cnil.fr*

Microsoft, IBM & Palo Alto Networks. (s.f.). Whitepaper: Modern SOC. *https://www.microsoft.com/security/blog*, *https://www.ibm.com/security/soc*, *https://www.paloaltonetworks.com/resources*

European Parliamentary Research Service (EPRS). (s.f.). La IA en la ciberseguridad europea. *https://www.europarl.europa.eu/thinktank*

Instituto Nacional de Ciberseguridad (INCIBE). (2023). Guía de continuidad de negocio para pequeñas y medianas empresas. *https://www.incibe.es*

Centro de Ciberseguridad Industrial (CCI). (2022). Modelo de madurez de capacidades de seguridad para entornos industriales. *https://www.cci.es*

Centro de Ciberseguridad Industrial (CCI). (2022). Guía de automatización de procesos en ciberseguridad. *https://www.cci.es*

MITRE Corporation. (s.f.). ATT&CK Framework. *https://attack.mitre.org*

Red Canary. (s.f.). Atomic Red Team. *https://atomicredteam.io*

European Union Agency for Cybersecurity (ENISA). (2021). Threat Landscape. *https://www.enisa.europa.eu/publications/threat-landscape*

Gartner. (2020). Innovation Insight for Extended Detection and Response. *https://www.gartner.com/en/documents/3984231*

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. *https://www.nist.gov/cyberframework*

SANS Institute. (s.f.). Security Operations Center: Functions and Capabilities. *https://www.sans.org*

IBM X-Force. (2022). Cyber Resilient Organization Study. *https://www.ibm.com/security/xforce*

World Economic Forum. (2021). Principles for Board Governance of Cyber Risk. *https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk*

Healthcare Information and Management Systems Society (HIMSS). (2021). Cybersecurity in Healthcare: A HIMSS Survey Report. *https://www.himss.org/resources/cybersecurity-healthcare*

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). Convocatorias para Compra Pública Innovadora. Retos relacionados con SOCs sectoriales *https://www.incibe.es/industria-cpi/cpi-segunda-convocatoria*


isms
forum
CSC
CYBER SECURITY CENTRE