

SOC (Security Operations Center)

CENTRO DE OPERACIONES DE SEGURIDAD

Los Centros de Operaciones de Seguridad (SOC)

Surgen ante la necesidad de **profesionalizar y sistematizar** las funciones de seguridad en las organizaciones. Se parecen bastante a los **NOC (Network Operations Centers)**, que son centros encargados de gestionar redes, pero los SOC están **orientados exclusivamente a la seguridad de la información**.

Un SOC puede ser interno o **una empresa externa especializada**, contratada para prestar este servicio. Esto ocurre, sobre todo, en **empresas** cuyo **giro principal no es la tecnología**, por lo tanto, **no tienen ni personal ni infraestructura especializada en seguridad informática**.

*En este modelo, **se transfiere la responsabilidad de proteger los activos digitales a una entidad externa**, algo similar al esquema de outsourcing:*

"No contrato directamente al personal ni mantengo la infraestructura, pero garantizo el servicio especializado mediante un proveedor."

*Esto **permite reducir costos**, ya que formar y mantener un equipo altamente capacitado, junto con herramientas avanzadas, puede resultar muy costoso. En cambio, **una empresa externa ya dispone de recursos humanos y tecnológicos adecuados**, y puede prestar este servicio a múltiples clientes.*

Ahora bien, **para que este modelo funcione** correctamente, **es fundamental establecer condiciones contractuales claras**:

- **Certificar que el personal esté realmente calificado.**
- **Asegurar la disponibilidad de herramientas tecnológicas necesarias.**
- **Establecer acuerdos de nivel de servicio (SLA).**

En nuestro entorno local, **los SOC se han vuelto cada vez más comunes**. Incluso tenemos **egresados de esta facultad que ya están trabajando en SOC**s, algunos de ellos sin salir de casa:

Acceden remotamente a los paneles de monitoreo, herramientas y sistemas de los clientes asignados, gestionando turnos e incidentes desde sus hogares.

Por tanto, **un SOC no siempre es una sala física llena de pantallas**: puede funcionar de forma completamente distribuida con personal remoto.

Definición general de SOC:

▪ Un centro de operaciones de seguridad, a menudo denominado SOC, es una **sede centralizada**, ya sea un lugar **físico** real o una organización **virtual**, **para monitorear, detectar y responder a problemas de seguridad e incidentes que pueda enfrentar una empresa**. Existen varios modelos para implementar un SOC como parte de **un programa más** grande de **Detección y Respuesta a Incidentes (IDR)**, que incluye modelos internos, modelos co-gestionados y modelos totalmente administrados o subcontratados.

▪ Puede pensar en un centro de operaciones de seguridad como una **sala de guerra** de películas estereotipadas: una habitación oscura llena de mapas complejos, monitores sofisticados y analistas en los auriculares. Sin embargo, la mayoría de los SOC no son realmente una habitación física; más exactamente, son un equipo formalmente organizado que está **dedicado a un conjunto específico de roles de seguridad y responsabilidades para detectar y validar amenazas dentro de su entorno**.



En cuanto al enfoque, el SOC **forma parte** del **equipo azul (Blue Team)** en ciberseguridad, cuya misión es:

- **Monitorear.**
- **Detectar.**
- **Analizar.**
- **Responder a incidentes.**

Esto se enmarca en la defensa activa de la organización frente a amenazas.

Un **SOC (Security Operations Center)** es una **unidad especializada, interna o externa**, encargada de **monitorear, detectar, gestionar y responder** a incidentes de seguridad informática, con el objetivo de proteger los activos digitales de una organización.

Una organización dedicada a la ciberseguridad —como un SOC— **realiza todo el trabajo de vigilancia y protección de los activos digitales** de una empresa. Pero para que esto sea efectivo, **la propia empresa debe haber definido previamente qué activos son los más valiosos y qué desea proteger**. Esta protección, por supuesto, implica una inversión.

Actividades en un SOC

Respuesta a Incidentes

Un SOC puede integrarse como parte de **un programa más amplio de gestión de detección y respuesta ante incidentes**. Dentro de esta estructura, es común encontrar la formación de equipos específicos como los **CSIRT (Computer Security Incident Response Teams)**, que veremos más adelante. Estos **se encargan de responder a incidentes**, mientras que los **equipos azules** se enfocan en la **vigilancia y monitoreo continuo**.

Las actividades de estos equipos **dependen del tipo de empresa y del entorno donde operan**, pero **son especialmente importantes en países o sectores con infraestructuras críticas** (como energía, banca, salud, transporte, etc.) o en empresas que valoran su **propiedad intelectual y activos digitales**, como ocurre con industrias altamente reguladas.

Ataques modernos

- Los ataques cibernéticos no son nuevos, pero ahora los adversarios son más sofisticados, cuentan con más recursos, están **capacitados y son adeptos a lanzar campañas de intrusión hábilmente planificadas llamadas Amenazas Persistentes Avanzadas (APT)**.
- La seguridad y la prosperidad de una **nación dependen de la infraestructura crítica**. Proteger estos activos requiere una comprensión clara de los adversarios, sus motivaciones y estrategias.

Una de las **amenazas más peligrosas** que deben enfrentar estos equipos son las llamadas **APT (Amenazas Persistentes Avanzadas)**. Estas amenazas:

- **Emplean técnicas de intrusión sofisticadas.**

- Utilizan malware especializado y exploits dirigidos.
- Se caracterizan principalmente por su **persistencia**.

¿Qué entendemos por *persistencia*?

Significa que **una vez que el atacante ha logrado el acceso, permanece dentro del sistema durante semanas o incluso meses**, sin ser detectado. No se trata de un ataque rápido y puntual, sino de una **presencia encubierta y sostenida**, lo que los hace **extremadamente peligrosos**.

Por eso, **muchas organizaciones descubren que han sido comprometidas meses después**, cuando se filtra información confidencial, bases de **datos de clientes, patentes o correos electrónicos**. En esos casos, el daño ya está hecho.

Ciclo OODA

Para **enfrentar** estas **amenazas se utilizan dos enfoques clave**:

Uno de ellos proviene del **ámbito militar** y es conocido como el **Ciclo OODA**, desarrollado por el estratega **John Boyd**. Este ciclo, aunque originalmente militar, **se aplica hoy en ciberseguridad y gestión de incidentes**. Sus fases son:

- **O (Observe)**: Observar, recopilar información, analizar el entorno.
- **O (Orient)**: Orientar, es decir, dar dirección con base en lo observado.
- **D (Decide)**: Tomar decisiones informadas.
- **A (Act)**: Actuar según el plan definido.

Este ciclo se repite constantemente, lo que permite a los equipos adaptarse rápidamente a amenazas nuevas o persistentes.

- El ciclo OODA es una **metodología que aborda el tratamiento de problemas o incidentes**. El concepto fue desarrollado por primera vez por el estratega militar y Coronel de la USAF John Boyd. El Coronel Boyd creó un enfoque de **cuatro pasos** diseñado para determinar la respuesta adecuada a un problema. El ciclo OODA, consta de los siguientes pasos: **observar, orientar, decidir y actuar**.

Fuente: <https://psychsafety.com/john-boyd-and-the-ooda-loop/>

- **Observe:** monitoree, recopile y almacene datos de varios puntos de su red como el primer paso en el ciclo OODA.
 - **Orientar:** analice los datos recopilados en busca de actividades sospechosas. Esto usualmente implica el uso de herramientas para procesar y analizar datos entrantes y almacenados.
 - **Decidir:** determinar un curso de acción basado en los resultados de la fase de análisis y la experiencia que ha obtenido de iteraciones de bucle anteriores.
 - **Actuar:** ejecuta el curso de acción que se determinó en el paso anterior.
- El ciclo OODA fue diseñado para hacer frente a ataques militares, pero los conceptos se aplican a la defensa de cualquier forma de ataque, incluidas las amenazas cibernéticas.

Cuando hablamos de tomar decisiones y ponerlas en ejecución, nos referimos a la aplicación práctica del ciclo OODA. Es decir:

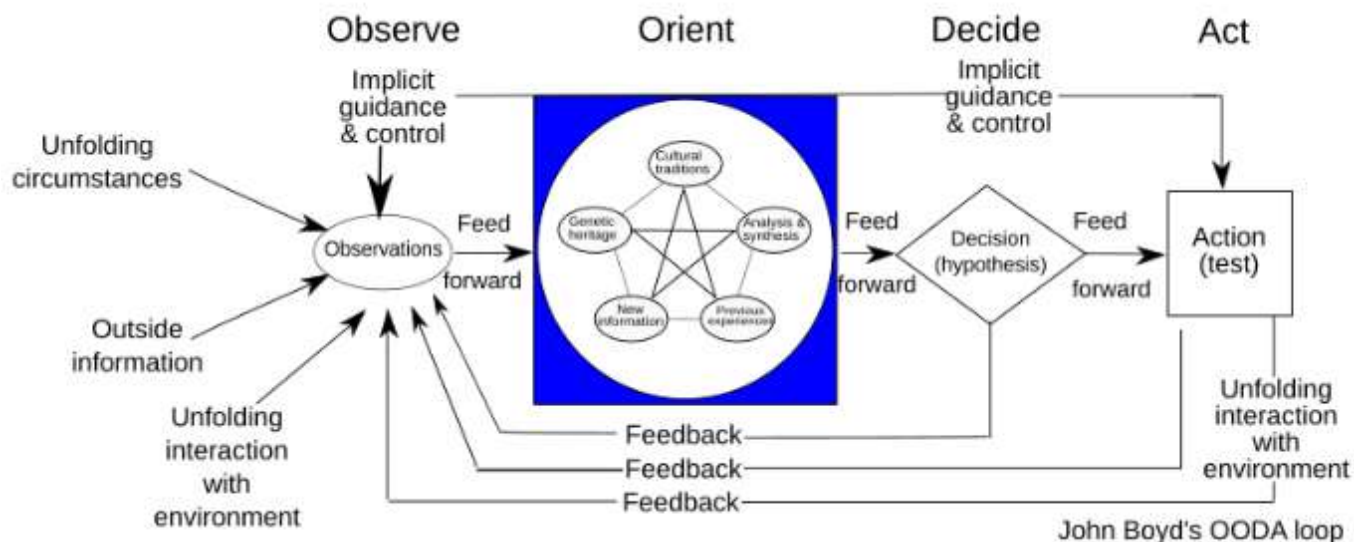
- **Observar** equivale a **monitorear y recopilar información** relevante en tiempo real.
- Para ello, **es indispensable contar con sensores** distribuidos en la red. Por sensores entendemos:
 - **Registros de logs** correctamente activados y almacenados.
 - **Agentes de antivirus.**
 - **Sistemas IDS/IPS.**
 - **Herramientas SIEM**, entre otros.

Si no existe esta base informativa, es imposible detectar comportamientos anómalos, intentos de acceso indebido o tráfico malicioso. Y esto es clave: **no se puede proteger lo que no se puede ver.**

Además, dada la **enorme cantidad de registros** que puede generar incluso una sola máquina (como vimos en el ejemplo de los logs en un sistema Windows), **es inviable hacer este trabajo de forma manual.** Se necesitan herramientas automatizadas que:

- Recopilen,
- Filtren,
- Analicen,
- Y visualicen la información de manera comprensible.

Con base en esa información, se toman decisiones: ¿qué acción seguir? ¿Se trata de una amenaza? ¿Se requiere bloqueo inmediato? ¿Se escala el incidente?



La imagen representa el **OODA Loop**, un modelo desarrollado por el coronel John Boyd, diseñado para describir cómo los seres humanos o las organizaciones toman decisiones en contextos dinámicos y cambiantes. El ciclo está compuesto por cuatro fases: **Observar, Orientar, Decidir y Actuar**. Estas etapas no ocurren de manera lineal y aislada, sino que están interconectadas mediante flujos de información, retroalimentación constante y mecanismos de guía implícita. Es un modelo especialmente útil en situaciones que requieren rapidez, adaptación y ventaja competitiva.

La primera fase, **Observar**, consiste en recopilar toda la información posible sobre el entorno, incluyendo circunstancias que se están desarrollando, interacciones con el ambiente y datos provenientes del exterior. El propósito es tener una imagen clara de la situación actual. Esta información se transforma en observaciones que alimentan el resto del proceso.

La segunda fase, **Orientar**, es la más crítica y compleja del modelo. En ella, el individuo o grupo interpreta lo observado basándose en varios factores como la herencia genética, las tradiciones culturales, la experiencia previa, la nueva información disponible y el proceso mental de análisis y síntesis. Todos estos elementos influyen en cómo se entiende la situación y qué opciones parecen viables. Es aquí donde se forma el marco mental desde el cual se tomarán decisiones.

En la fase de **Decidir**, se formula una hipótesis o plan de acción, basada en la orientación previa. Esta decisión representa una elección entre posibles cursos de acción. La decisión no se ejecuta inmediatamente de forma aislada, sino que también puede verse influenciada por una guía implícita y por la retroalimentación continua del entorno.

La fase final es **Actuar**, donde se ejecuta la decisión tomada. Esta acción produce una nueva interacción con el entorno, lo que genera más información para reiniciar el ciclo. El resultado de la acción permite comprobar si la hipótesis fue correcta o no, lo que retroalimenta al sistema y ajusta los pasos siguientes.

Este modelo se repite constantemente y su eficacia depende de cuán rápido y correctamente se ejecute el ciclo frente a los cambios del entorno. En contextos como la guerra, los negocios o la seguridad informática, quien recorre el ciclo más rápido puede adaptarse mejor y superar a sus competidores o adversarios.

Esto nos lleva a otro aspecto importante: **la experiencia del analista**. Esta puede marcar la diferencia entre detectar una intrusión a tiempo o dejar pasar un ataque crítico. No basta con tener datos y herramientas, también se necesita criterio para interpretar lo que se está viendo.

En el contexto empresarial, especialmente en sectores como la banca, cuando ocurre una filtración o un **incidente grave**

*—como ha sucedido con el Banco Interbank, por ejemplo—, **la respuesta institucional es inmediata**: se despide a los responsables, desde jefes de seguridad hasta personal técnico. Esto demuestra que, cuando fallan los controles, **la responsabilidad recae en quienes debían tomar decisiones oportunas con la información disponible**.*

Eso es lo que hacen muchas empresas: desvinculan al personal tras un incidente. Pero no consideran que ese mismo personal ha adquirido una experiencia valiosa que podría ser aprovechada para prevenir futuros incidentes.

Claro, esa experiencia puede haber costado mucho dinero. Y justo a ese punto quería llegar. El valor está en comprender que, si bien un incidente puede generar pérdidas millonarias, no se trata de promover errores para aprender, sino de reconocer que **la experiencia adquirida en situaciones críticas es insustituible**.

No estoy diciendo que debamos permitir que ocurran fallas graves para formar al personal, pero cuando estas situaciones ocurren —porque inevitablemente suceden en cualquier entorno tecnológico— **el enfoque no debe ser solo punitivo**, sino también formativo. El problema es que, al despedir de inmediato a los responsables, **la empresa pierde esa experiencia**, que probablemente será aprovechada por otra organización. Es decir, no se trata de que la empresa fomente errores, sino de que **evalúe con criterio la naturaleza del incidente**: ¿fue una omisión leve o una negligencia grave e imperdonable? En algunos casos, ni siquiera otro profesional con más experiencia habría podido actuar mejor, quizás por tratarse de un ataque nuevo, una vulnerabilidad sin parches o por falta de recursos clave. ¿Tenía el administrador las herramientas necesarias? ¿Se le negó presupuesto o acceso a tecnologías que solicitó con anticipación?

Por eso, más allá de los detalles específicos, **la experiencia en la toma de decisiones bajo presión es vital**, y puede marcar la diferencia. Eso aplica no solo a la seguridad informática, sino a muchos ámbitos profesionales. Pero en ciberseguridad, donde un error puede afectar a millones, esta capacidad es crítica.

—Por otro lado competencias tipo *Capture the Flag* (CTF) usando plataformas como *Hack The Box*, *TryHackMe* o *Root-Me*. Esas experiencias —aunque sean simuladas— también son una excelente forma de entrenarse y ganar criterio para responder a situaciones reales.

¿Qué son las CTF (Entrenamiento en Seguridad Ofensiva)?

¿Dónde resolvías máquinas o problemas? ¿Alguien ha jugado o ha entrado a **Hack The Box (HTB)** alguna vez? ¿Han escuchado de eso?

Si no, les explico: plataformas como **HTB** o **TryHackMe** permiten participar en retos llamados **CTF** (*Capture The Flag*), que nacieron en el ámbito **militar** y se trasladaron al mundo de la **seguridad informática**.

Un **CTF** es una **competencia por equipos** en la que se deben encontrar "**flags**" (banderas), las cuales son fragmentos de texto ocultos dentro de sistemas o servicios simulados. Por ejemplo, una bandera puede estar en el directorio home de un usuario en un servidor Linux detrás de una red y firewall.

Estas competencias ofrecen **escenarios simulados**, con **entornos no reales**, lo cual permite:

- Aprender y practicar con **herramientas reales** de hacking ético.
- Identificar y **explotar vulnerabilidades**.
- Simular situaciones sin riesgos para entornos productivos (empresas, bancos, universidades, etc.).

Aquí en la facultad, organizamos un par de **competencias internas CTF** antes de la pandemia, como parte de las celebraciones de aniversario. En ellas, los equipos tenían que **escalar privilegios**, **romper firewalls** y **llegar a la bandera final**.

Ahora, **¿cuál es el problema de solo tener experiencia en CTF?**

*Supongamos que una persona, brillante en **Hack The Box**, fue contratado para su primera auditoría de pentesting real en una red de una empresa. ¿Qué hizo? Lanzó un escaneo agresivo de inmediato. Esto generó un problema contractual serio, porque esa infraestructura era sensible al alto tráfico. El entorno productivo no es un laboratorio, y no se puede aplicar el mismo enfoque agresivo de las competencias sin consecuencias.*

Este caso nos deja una lección clave:

Puedes tener **conocimientos técnicos**, saber usar **herramientas como Nmap, Burp o Metasploit**, pero **sin experiencia real**, podrías tomar decisiones **catastróficas**.

En un CTF importa la **velocidad** y **agresividad**; en el mundo real importa la **precisión**, el **análisis de riesgos**, y el **impacto** de tus acciones. No estás jugando: estás tratando con datos reales, infraestructuras críticas y servicios que no pueden fallar.

Tener técnica **sin criterio ni experiencia** puede ser peligroso.

Por eso, en seguridad informática es tan importante **complementar la teoría con la práctica profesional responsable**. Tomar malas decisiones técnicas puede llevar a consecuencias serias. La **formación integral** incluye **saber cuándo actuar, cómo actuar**, y sobre todo, **cuánto impacto puede tener tu acción** en entornos reales.

Cuando una **acción falla o no funciona** como se espera, entramos en un **ciclo de retroalimentación**.

¿Qué es este ciclo?

El proceso de toma de decisiones en seguridad **no es lineal**, sino **iterativo**. Es decir, **se puede volver atrás** en cualquier punto:

- Si estás en la etapa de **decisión**, pero **no estás seguro**, puedes **regresar a observar o recopilar nuevos datos**.
- Si una **nueva información aparece**, puede **cambiar tu decisión** y, por tanto, tu **curso de acción**.

En el ejemplo anterior del escaneo agresivo, se perdieron servicios críticos por una mala decisión. ¿Qué se aprendió?

- El analista aprendió que **no puede aplicar técnicas agresivas** sin evaluación previa del entorno.
- La **empresa también falló**, al **no verificar** si el personal tenía la **experiencia real**, más allá de sus **certificaciones**.

◆ **Certificación** ≠ **Experiencia** **práctica**
◆ **Inducción técnica y normas claras** son clave antes de ejecutar pruebas de seguridad.

👁 **Observación en Seguridad: ¿De dónde viene la información?**

La **observación** puede provenir de cualquier fuente:

- **Usuarios**
- **Clientes**
- **Máquinas**
- **Logs**
- **Sistemas de detección (IDS, antivirus, etc.)**

Incluso **reportes de usuarios** sobre actividades sospechosas **deben ser tomados en cuenta**. Sin embargo, si **no hay protocolos ni roles definidos**, esta información **no se procesa correctamente**.

Caso Real: Prueba de Ingeniería Social

Se realizó un ejercicio de **tesis** en el que estudiantes simulaban ser practicantes y **se infiltraron en oficinas administrativas**. ¿Qué se observó?

- **Muy pocas personas alertaron.**
- Algunas **sí reportaron el hecho**, pero **no hubo una acción organizada**.
- **No existía un protocolo** activado ni un **oficial de seguridad** que respondiera.

Esto demuestra que **sin procesos definidos**, la información **se pierde o no se considera relevante**.

Los ataques como el **phishing telefónico** funcionan porque:

- En muchas empresas **no se conoce personalmente** al personal técnico.
- Es más fácil suplantar identidades cuando los empleados **no saben quiénes integran el equipo de soporte**.

En entornos donde "todos se conocen", como en un equipo pequeño o una universidad, es **más difícil suplantar** a alguien. Pero en organizaciones grandes o tercerizadas, **el atacante tiene más ventaja**.

Orientación Defensiva Basada en Información y Experiencia

Una vez recopilada la información durante la **fase de observación**, el siguiente paso es **orientarse**:

- Analizar la información.
- Compararla con **experiencias previas o casos similares**.
- Hacer un **benchmark** con otros incidentes.
- Formular una **hipótesis** que permita **decidir** el mejor curso de acción.

Cadena de la Muerte (*Kill Chain*)


- Para nuestro próximo modelo, cambiamos al punto de vista del atacante y observamos la cadena de ciberataque o cadena de la muerte (*kill chain*). La cadena cibernética, desarrollada por el equipo de respuesta a incidentes informáticos de Lockheed Martin, describe la progresión que sigue un atacante al planear y ejecutar un ataque contra un objetivo. Este modelo ayuda a los profesionales de seguridad a identificar los controles de seguridad y las acciones que pueden implementarse o mejorarse para detectar, denegar y contener un escenario de ataque

La Cadena de la Muerte (Cyber Kill Chain)

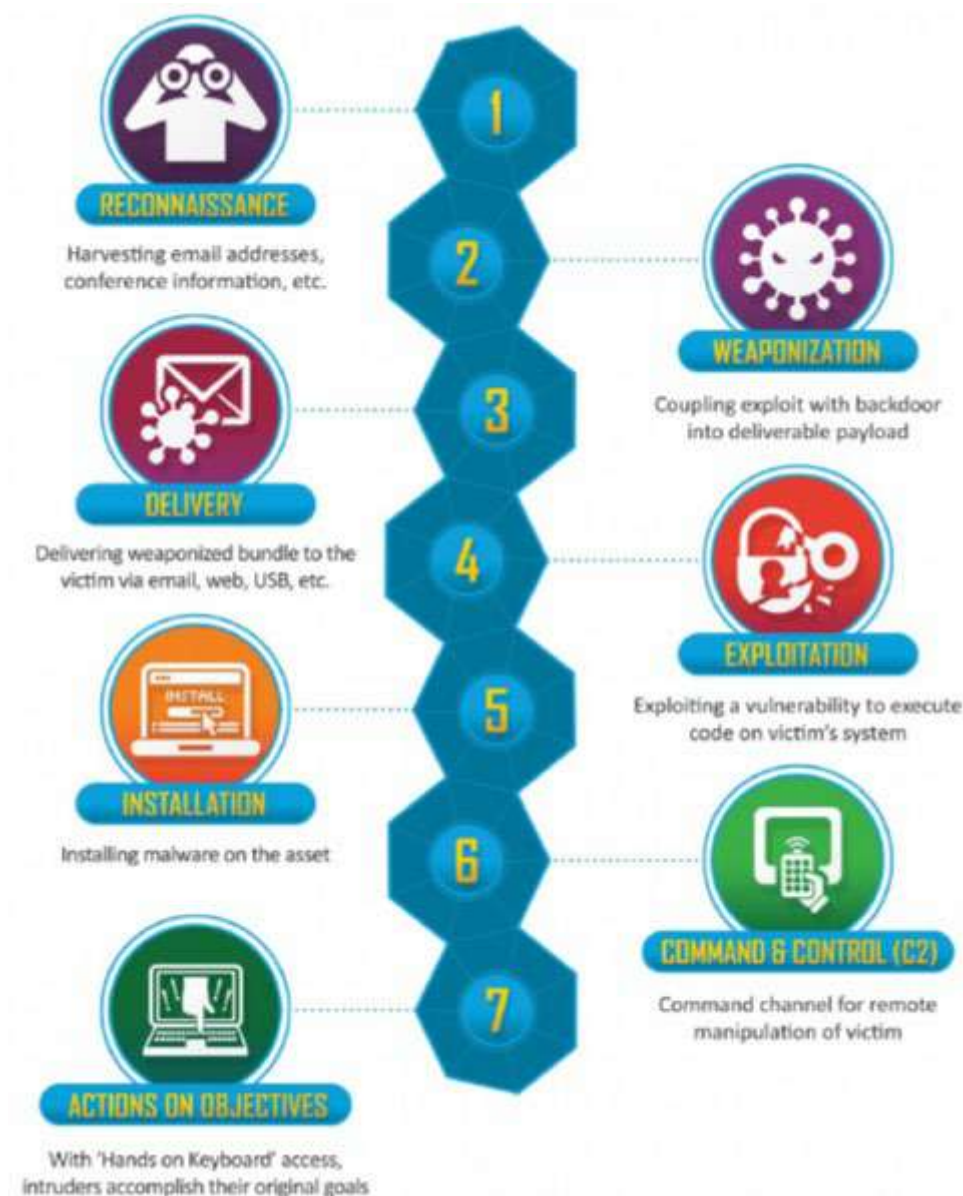
Este modelo proviene del ámbito militar (Lockheed Martin) y se adapta a la **ciberseguridad ofensiva y defensiva**.

Consiste en **7 etapas** que suelen seguir los atacantes:

1. **Reconocimiento**
2. **Armamento**
3. **Entrega**
4. **Explotación**
5. **Instalación**
6. **Comando y control**
7. **Acciones en el objetivo**

 Desde el **punto de vista defensivo**, esta cadena ayuda a **anticipar los pasos del atacante** y definir **controles específicos por cada etapa**.

! *Advertencia:* Este modelo **no garantiza detener todos los ataques**, pero **ayuda a entender cómo piensan los atacantes** y a fortalecer nuestras defensas en puntos críticos.



Etapa 1: Reconocimiento (Reconnaissance)

Tanto **atacantes como defensores** deben realizar reconocimiento. Los **malos buscan**:

- Correos electrónicos del personal.
- Dominios públicos.
- Estructura organizacional.
- Información de usuarios en redes (LinkedIn, Facebook).

Los **defensores deben identificar** qué información está expuesta y:

- Reconocer qué datos **no se pueden eliminar** (como publicaciones pasadas o fotos).
- Mitigar su utilidad para el atacante.

💡 **Ejemplo práctico:** Un ciberdelincuente busca perfiles de empleados en LinkedIn y encuentra correos electrónicos y detalles de cargos para preparar ataques personalizados (spear phishing).

📖 **Ataque a Sony Pictures (2014):** Los atacantes norcoreanos buscaron correos electrónicos de empleados y vulnerabilidades en sus servidores antes de lanzar el ataque.

📖 **Campaña APT28 (Fancy Bear):** Recopilaron información pública y privada sobre funcionarios de la OTAN para ataques de phishing.

📖 **Ataques a hospitales (2021):** Actores de ransomware escanean sistemas expuestos (como RDP) para identificar blancos vulnerables.

🛑 ¿Qué Hacer con Información Expuesta?

Hacer que **la información pública o filtrada sea inútil** para planear un ataque. Algunas estrategias sugeridas:

🔒 1. Inutilizar credenciales filtradas

- Si una contraseña está comprometida, **prohibir su uso** dentro de la organización.
- Aplicar **listas negras de contraseñas**.

👤 2. Reducir el perfil público

- Evitar que personal clave publique en exceso sobre sus cargos y funciones.
- Fomentar el uso de redes profesionales con **perfiles moderados**.

✉️ 3. Correo institucional anonimizado

- Usar **códigos internos** en lugar de nombres reales.
- Ejemplo: en lugar de `juan.perez@empresa.com`, usar `us001@empresa.com`.

📜 4. Compromisos contractuales

- Hacer que el personal firme una **declaración jurada** sobre el uso responsable de su información en redes.
- Establecer **sanciones** si exponen datos sensibles o estratégicos de forma pública.

La pregunta clave del ejercicio fue:

¿Qué acciones tomarías si eres responsable de ciberseguridad y descubres que tus analistas están muy expuestos en redes sociales?

Algunas ideas que surgieron:

- **Ocultar nombres reales** mediante alias o códigos en plataformas públicas.
- Mantener las **cuentas personales separadas** de las institucionales.
- Configurar **alertas de exposición** mediante herramientas de monitoreo de OSINT (como Shodan o Maltego).

En muchos casos, el **personal de una organización** publica en sus redes sociales información como:

- Lugar de trabajo.
- Cargo específico (ej. *Administrador de red*).
- Herramientas que usan (ej. *Huawei, Cisco*).
- Certificaciones.
- Teléfono y correo institucional.

Esta información puede ser usada por atacantes para **diseñar ataques de ingeniería social personalizados** y altamente efectivos.

¿Por qué es tan peligrosa esta información? Porque le permite al atacante:

- **Construir un perfil** detallado de la víctima.
- Inferir qué tecnologías usa la empresa.
- Saber **quién tiene acceso privilegiado**.
- Planificar **phishing dirigido**, llamadas falsas (vishing) o suplantación de identidad.



¿Cómo se puede contrarrestar esta exposición?

1. Políticas claras de uso de redes sociales

- Establecer normativas internas para **limitar la publicación** de información sensible.
- Prohibir publicaciones que revelen detalles operativos, cargos técnicos o accesos.



Ejemplo: No permitir que se publique “Administrador de servidores Huawei – Empresa XYZ”.

2. Uso de alias o codificación

- En vez de correos como `juan.perez@empresa.com`, usar formatos del tipo `user045@empresa.com`.
- **Enmascarar nombres** en sitios públicos como LinkedIn con descripciones genéricas: “Área Técnica” en lugar de “Administrador de Red”.

3. Entrenamiento y sensibilización

- Capacitar al personal en:
 - Identificación de ataques de ingeniería social.
 - Buenas prácticas en la gestión de su imagen digital.
 - **Conciencia de ciberseguridad personal e institucional.**



Contramedida clave: No puedes evitar que se expongan, pero sí puedes **entrenarlos para que no caigan.**

4. Simulacros de ataque (Red Team – Blue Team)

- Realizar ejercicios de phishing simulado y ataques controlados para medir la respuesta del personal.
- Retroalimentar con análisis y recomendaciones.

5. Gestión proactiva de identidades

- Implementar políticas de **mínimo privilegio** y rotación de credenciales.
- Utilizar **sistemas de doble autenticación (2FA)** para proteger accesos incluso si se expone una contraseña.



En resumen

La información expuesta no siempre se puede borrar.
Pero sí se puede hacer que no sea útil para un atacante.

¿Cómo?

- Entrenando a las personas.
- Controlando qué y cómo se publica.
- Aplicando controles técnicos y organizativos.



Simulacros de Phishing y Defensa Corporativa




Objetivo: Preparar al Usuario, No Solo la Infraestructura

En el marco de las pruebas de seguridad, muchas empresas implementan **ejercicios anuales de phishing** como parte de sus **programas de capacitación y entrenamiento**. El objetivo principal no es probar las defensas tecnológicas como los filtros de correo, sino **evaluar el comportamiento del usuario** ante amenazas realistas.

¿Cómo se realizan las pruebas de phishing?

Tipos de prueba:

- **Contra la tecnología:** Evaluar filtros de spam (NO es el enfoque aquí).
- **Contra el usuario:** Evaluar si cae ante un correo convincente (SÍ es el enfoque).

 Se asume una *intrusión ya lograda* (bypass) para simular qué pasaría si el correo malicioso llega a la **bandeja de entrada**, no al spam.

Desafío técnico:

- Google y Microsoft tienen **filtros de seguridad**.
- Para evitar bloqueos, se debe colocar el dominio o IP del phishing en la **lista blanca temporalmente**.

Preparación del escenario


Tematización del ataque

Los *phishing* deben adaptarse al **contexto real de la empresa**:

- Ejemplo: si el *Día de la Madre* está cerca, se puede crear un correo que ofrezca una promoción o sorteo usando un restaurante proveedor de la empresa.
- Este enfoque **aumenta la credibilidad** del mensaje y la probabilidad de que el usuario haga clic.

Técnicas utilizadas:

- Formularios falsos que simulan recoger **datos personales o credenciales**.
- Páginas clonadas que simulan plataformas reales.
- Correos con **archivos adjuntos** o enlaces maliciosos.

 Hoy en día, lograr que el usuario *ingrese su contraseña* en un formulario requiere más sofisticación, pero aún es posible si se simula acceso a sistemas que conoce.

Fases del Ataque según la Cadena de la Muerte (*Cyber Kill Chain*)

1. Reconocimiento

Recopilación de información pública:

- Tecnologías utilizadas (Google, Microsoft).
- Proveedores, fechas especiales.
- Correos corporativos o estilos de comunicación.

Objetivo: recolectar información sobre la víctima.

1. **Ataque a Sony Pictures (2014):** Los atacantes norcoreanos buscaron correos electrónicos de empleados y vulnerabilidades en sus servidores antes de lanzar el ataque.
2. **Campaña APT28 (Fancy Bear):** Recopilaron información pública y privada sobre funcionarios de la OTAN para ataques de phishing.
3. **Ataques a hospitales (2021):** Actores de ransomware escanean sistemas expuestos (como RDP) para identificar blancos vulnerables.

■ **Fase 1: Reconocimiento.** El atacante recopila información sobre el objetivo antes de que comience el ataque real. Puede hacerlo buscando información públicamente disponible en Internet.

2. Armado (Weaponization)

- Se crea el **código malicioso** o *exploit* (payload).
- Basado en lo aprendido del entorno tecnológico de la empresa.
- Preparación de archivos, páginas falsas o correos.

Objetivo: crear una carga útil maliciosa.

1. **Stuxnet (2010):** Se empacó un exploit de día cero junto a un rootkit que atacaba sistemas SCADA.
2. **APT10 (Cloud Hopper):** Usaron documentos Word con macros maliciosas para instalar puertas traseras.
3. **Campaña Emotet:** Combinaban documentos de Word con scripts de PowerShell para instalar malware bancario.

■ **Fase 2: Armamento o armado.** El atacante usa un *exploit* y crea una carga maliciosa para enviar a la víctima. Este paso ocurre en el lado del atacante, sin contacto con la víctima.

3. Entrega (Delivery)

Métodos comunes:

- Correo electrónico (*phishing*).
- Sitios web comprometidos.
- Dispositivos USB infectados.
- Canales físicos o digitales.



Ejemplo: el ataque *Stuxnet* a una planta nuclear fue iniciado mediante un USB infectado.

Objetivo: hacer llegar el malware a la víctima.

1. **WannaCry (2017):** Se propagó a través de una vulnerabilidad en SMBv1 en redes Windows.
2. **Correo falso de la OMS (COVID-19, 2020):** Campañas de phishing entregaron malware haciéndose pasar por recomendaciones sanitarias.
3. **USBs infectados en universidades:** Dejaban USBs físicamente en estacionamientos; los usuarios curiosos los conectaban y ejecutaban malware.

▪ **Fase 3: Entrega.** El atacante envía la carga maliciosa a la víctima por correo electrónico u otros medios, que representa uno de los muchos métodos de intrusión que el atacante puede usar.

4. Explotación

Se ejecuta el código malicioso aprovechando una **vulnerabilidad**, logrando:

- Inyección del malware.
- Apertura de una **conexión** al sistema comprometido.
- Inicio del proceso de instalación de más código malicioso.

Objetivo: ejecutar el código malicioso en el sistema víctima.

1. **EternalBlue (WannaCry/NotPetya):** Explotaron una vulnerabilidad en Windows para ejecutar malware sin intervención del usuario.
2. **Equifax (2017):** Usaron una falla en Apache Struts para ejecutar código remotamente y acceder a datos sensibles.
3. **Zero-day en Zoom (2020):** Vulnerabilidades permitieron ejecutar código remoto en sesiones de videollamada.

- **Fase 4: Explotación.** La ejecución real del *exploit*, que nuevamente es relevante solo cuando el atacante usa un *exploit*.

5. Instalación

- Se instalan **agentes persistentes** que permiten al atacante mantenerse conectado.
- Se descargan herramientas adicionales (malware, keyloggers, etc.).

Objetivo: establecer persistencia en el sistema.

1. **Troyano Zeus:** Instalado para robar credenciales bancarias mediante inyección en navegadores.
2. **RATs (Remote Access Trojans) como DarkComet:** Se instalan para controlar remotamente PCs durante meses.
3. **Malware en SolarWinds (2020):** El código malicioso se instaló como una actualización de software legítimo.

- **Fase 5: Instalación.** La instalación de malware en la computadora infectada es relevante solo si el atacante utilizó malware como parte del ataque, e incluso cuando hay malware involucrado, la instalación es un punto en el tiempo dentro de un proceso de ataque mucho más elaborado que lleva meses en operar.

6. Command & Control (C2)

- El atacante **mantiene el control** remoto sobre el sistema.
- Puede emitir órdenes, transferir archivos, o ampliar el acceso a otros sistemas.

Objetivo: comunicarse con el malware y controlarlo remotamente.

1. **Botnets como Mirai:** Dispositivos IoT infectados reciben comandos para realizar ataques DDoS.
2. **APT29 (Cozy Bear):** Enviaban comandos cifrados desde servidores externos para mantener persistencia.
3. **Cobalt Strike:** Herramienta legítima usada por atacantes para controlar hosts comprometidos desde un servidor C2.

- **Fase 6: Comando y Control.** El atacante crea un canal de comando y control para continuar operando de forma remota. Este paso es relativamente genérico y relevante durante todo el ataque, no solo cuando se instala malware.

7. Acción sobre el objetivo

- Robo de **información confidencial**.
- Sabotaje, cifrado de datos (*ransomware*), o espionaje continuo.
- Este es el **verdadero objetivo: acceder, exfiltrar o manipular datos** estratégicos.

Objetivo: cumplir con la meta del atacante.

1. **Robo de datos en Marriott (2018):** Filtraron información de más de 500 millones de huéspedes.
2. **Colonial Pipeline (2021):** Ransomware paralizó el suministro de combustible en EE.UU. y exigieron millonario rescate.
3. **Robo de secretos industriales por APT41 (China):** Accedieron a planos y diseños de múltiples empresas tecnológicas.

- **Fase 7: Acción sobre Objetivos.** El atacante realiza los pasos para lograr su objetivos reales dentro de la red de la víctima. Este es el elaborado proceso de ataque activo que lleva meses y miles de pequeños pasos para lograr.

Ataques Persistentes Avanzados (APT)

Objetivo real del atacante

Aunque la **explotación** (fase 4 del *Cyber Kill Chain*) es un hito técnico importante, **no es el objetivo final**. Lo que buscan los atacantes es:

- **Obtener réditos económicos**
- **Extorsionar** con datos robados
- **Vender información** sensible
- **Sabotear o destruir sistemas críticos**, especialmente en el caso de ataques patrocinados por **Estados-nación**

 Esto solo es posible si logran **mantener la persistencia** en los sistemas comprometidos.

¿Qué significa *persistencia*?

- Es **permanecer** dentro del entorno comprometido por semanas o incluso **meses**.
- Permite tener **varios accesos alternativos**: si uno falla, el atacante entra por otro.
- Se logra mediante técnicas de **Command & Control (C2)**.

Sin persistencia, una desconexión o reinicio del sistema puede hacer perder todo el acceso ganado.

MITRE ATT&CK

Modelo MITRE ATT&CK

¿Qué es?

Es una **matriz de conocimiento** basada en observaciones del mundo real sobre cómo actúan los atacantes. A diferencia del *Cyber Kill Chain* que describe las **etapas**, MITRE describe:

- **Tácticas**: los **objetivos** del atacante (ej. persistencia, escalada de privilegios, evasión).
- **Técnicas**: los **métodos específicos** para lograr esas tácticas.
- **Procedimientos**: ejemplos de cómo se usan esas técnicas en ataques reales.


PROBLEMAS QUE ABORDA MITRE ATT&CK

- **Comportamiento de adversarios**. Centrarse en las tácticas y técnicas del adversario permite desarrollar análisis para detectar posibles comportamientos del adversario. Los adversarios cambian fácilmente los indicadores típicos, como dominios, direcciones IP, hash de archivos, claves de registro, etc., y solo son útiles para una detección puntual; no representaban cómo los adversarios interactúan con los sistemas, solo que probablemente interactuaron en algún momento.
 - **Modelos de ciclo de vida que no encajan**. Los conceptos existentes del ciclo de vida del adversario y Cyber Kill Chain son de un nivel alto para relacionar los comportamientos con las defensas.
 - **Aplicabilidad a entornos reales**. Los TTP deben basarse en incidentes observados para demostrar que el trabajo es aplicable a entornos reales.
 - **Taxonomía común**. Los TTP deben ser comparables entre diferentes tipos de grupos adversarios utilizando la misma terminología.
-

Ejemplos de técnicas en MITRE

TÁCTICA	EJEMPLOS DE TÉCNICAS
ACCESO INICIAL	Spear phishing, USB infectado, credenciales robadas
EJECUCIÓN	Macros, scripts, PowerShell
PERSISTENCIA	Servicios maliciosos, modificación de registros
ESCALADA DE PRIVILEGIOS	Token hijacking, bypass de UAC
EVASIÓN DE DEFENSAS	Desactivación de antivirus, ofuscación
ACCESO A CREDENCIALES	Fuerza bruta, keyloggers
COMANDO Y CONTROL (C2)	Google Drive, Dropbox, canales cifrados
EXFILTRACIÓN	Transferencia por HTTP, DNS, almacenamiento en la nube

Ejemplo real:

 **Google Drive** y otros servicios cloud han sido usados como canales de entrega (*delivery*) de malware.

Esto permite evadir filtros convencionales de seguridad al tratarse de servicios aparentemente legítimos.

¿Realmente estos modelos detienen los ataques?

La respuesta es: **no completamente**.

- Estos modelos ayudan a **los defensores** a **entender, anticipar y mitigar** ataques conocidos.
- Pero **los atacantes no siguen necesariamente estas fases ni técnicas al pie de la letra**.
- De hecho, los atacantes más sofisticados **evitan comportarse como lo espera el modelo**.

El uso de MITRE o el *Kill Chain* no garantiza inmunidad, pero **sí mejora la capacidad de respuesta y preparación**.

La **comprensión de los modelos** como *Cyber Kill Chain* y **MITRE ATT&CK** permite:

- Identificar puntos vulnerables.
- Implementar **controles defensivos efectivos**.
- **Simular y preparar escenarios realistas** de intrusión.
- Entrenar equipos de respuesta para actuar en cada fase.

Sin embargo, **la adaptabilidad y creatividad de los atacantes** obliga a las organizaciones a **actualizar constantemente sus estrategias de defensa**.

Modelos de ataque: ¿Son infalibles?

¿Los atacantes siguen las etapas al pie de la letra?

No necesariamente.
Aunque los modelos como el **Cyber Kill Chain** o la matriz **MITRE ATT&CK** nos ofrecen una estructura lógica del comportamiento de un atacante, **no garantizan que los atacantes reales sigan exactamente esas etapas.**

De hecho:


- Muchos **saltan pasos.**
- Otros **actúan en desorden.**
- Algunos **usan técnicas nuevas** que no están registradas aún.

 **Los modelos ayudan, pero no previenen por sí solos los incidentes.**

MITRE ATT&CK y sus variantes

El framework MITRE no solo está enfocado en sistemas **Windows**. También ofrece matrices para:

- **Linux**
- **macOS**
- **Dispositivos móviles (Android/iOS)**
- **Ingeniería social**
- **Técnicas de phishing, spear phishing y otros vectores humanos**

 Hay documentación descargable y herramientas como **MITRE Engenuity** y simuladores de ataque (*tabletop exercises*) para preparar respuestas ante incidentes.

Matriz ATT&CK para Windows

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
9 techniques	10 techniques	18 techniques	13 techniques	34 techniques	15 techniques	25 techniques	9 techniques	15 techniques	16 techniques	8 techniques
Drive-by Compromise	Command and Scripting Interpreter (2)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Adversary in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (10)	Boot or Logon Autostart Execution (10)	Debugger Evasion	Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking (1)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel
Phishing (3)	Scheduled Task/Job (2)	Browser Extensions	Create or Modify System Process (1)	Direct Volume Access	Forge Web Credentials (2)	Domain Trust Discovery	Remote Services (3)	Browser Session Hijacking	Dynamic Resolution (2)	Exfiltration Over Other Network Medium (1)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (2)	Event Triggered Execution (11)	Execution Guardrails (1)	Modify Authentication Process (3)	Group Policy Discovery	Software Deployment Tools	Data from Information Repositories (1)	Failback Channels	Exfiltration Over Web Service (2)
Trusted Relationship	System Services (1)	Create or Modify System Process (1)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Network Service Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer
Valid Accounts (3)	User Execution (2)	Event Triggered Execution (11)	Hijack Execution Flow (16)	File and Directory Permissions Modification (1)	Multi-Factor Authentication Request Generation	Network Share Discovery	Use Alternate Authentication Material (2)	Data from Network Shared Drive	Multi-Stage Channels	
	Windows Management Instrumentation	External Remote Services	Process Injection (3)	Hide Artifacts (2)	Network Sniffing	Password Policy Discovery		Peripheral Device Discovery	Non-Application Layer Protocol	
		Hijack Execution Flow (16)	Scheduled Task/Job (2)	Hijack Execution Flow (16)	OS Credential Dumping (3)	Permission Groups Discovery (2)		Process Discovery	Non-Standard Port	
		Modify Authentication Process (3)	Valid Accounts (3)	Indicator Removal on Host (3)	Steal or Forge Kerberos Tickets (4)	Process Discovery		Query Registry	Protocol Tunneling	
		Office Application Startup (4)		Indirect Command Execution	Masquerading (3)	Remote System Discovery		Screen Capture	Proxy (4)	
		Pri-OS Boot (3)		Masquerading (3)	Modify Authentication Process (3)	Software Discovery (1)		Email Collection (3)	Remote Access Software	
		Scheduled		Modify Registry	Obfuscated Files or Information	System Information Discovery		Input Capture (4)	Traffic Signaling (1)	
				Obfuscated Files or Information		System Location		Video Capture	Web Service (3)	

Equipos de respuesta: CSIRT y CERT

¿Qué son los CSIRT/CERT?

- Son **equipos de respuesta a incidentes de seguridad informática**.
- Su misión es **detectar, contener, analizar y mitigar** amenazas.
- Están activos tanto en el sector público como privado.
- En países con **infraestructura crítica**, son esenciales para mantener la **ciberresiliencia nacional**.

¿Qué utilizan?

- **Modelos como MITRE ATT&CK**
- **Herramientas SIEM**
- **Análisis de indicadores de compromiso (IoC)**

Detección y Respuesta de Incidentes

- La detección y respuesta a incidentes de seguridad de la información es el núcleo de las operaciones de seguridad. Se espera que el equipo asignado a las operaciones de seguridad supervise los activos de la organización dentro del alcance y reaccione a los eventos e incidentes de seguridad, incluida la detección e investigación de lo que se considerarían **indicadores de compromiso (IOC)**.

Indicadores de compromiso (IoC)

¿Qué son?

Son **señales o evidencias técnicas** que indican que puede estar ocurriendo un incidente de seguridad.

Algunos ejemplos:

- Conexión inesperada de un **USB** en una máquina donde está **prohibido**.
- Intento de **autenticación remota** desde un dispositivo no reconocido.
- Acceso con **credenciales no utilizadas normalmente** o **provenientes de IPs sospechosas**.
- Cambios inusuales en el comportamiento de la red o del sistema.

¿Cómo se detectan?

Gracias al uso de:

- **Sistemas de monitoreo**
- **Análisis de logs**
- **Herramientas automatizadas de detección de anomalías**
- **Sensores distribuidos en los puntos críticos de la red**

 Detectar un IoC a tiempo puede evitar un ciberataque exitoso.

- Los **IOC** son señales de compromiso de seguridad técnica y no técnica que podrían detectarse con tecnología, procesos y personas. Por ejemplo, detectar a un usuario que accede a archivos desde un dispositivo de memoria USB en una computadora de escritorio empresarial puede indicar que se ha violado una política relacionada con la restricción del uso de dispositivos de memoria USB y que se ha eludido un control de seguridad. Otro ejemplo es la detección de la dirección IP de un servidor de comando y control de *botnet* de Internet dentro de su red que probablemente indique que uno o más de sus sistemas se han visto comprometidos.

- La respuesta a los incidentes comienza al detectar primero que un incidente realmente ha ocurrido y está dentro del alcance asignado al equipo de operaciones de seguridad. Un ejemplo es capturar algunas IOC con un sistema de monitoreo e investigando los eventos o entregando las tareas forenses a otros equipos o unidades.

El objetivo de los modelos y herramientas como **MITRE**, **CSIRT**, **SIEM**, entre otros, **no es eliminar el riesgo al 100%**, sino:

- **Reducir el impacto**
- **Aumentar la detección temprana**
- **Mejorar la respuesta ante amenazas**

La clave está en combinar **tecnología**, **procedimientos claros** y **personas capacitadas**.

🌟 Detección Basada en Comportamiento y Línea Base

Para que un sistema pueda identificar un **comportamiento inadecuado**, primero debe conocer cuál es el comportamiento **esperado** o normal. Por ejemplo, si se define que *todos los usuarios deben ingresar al sistema desde ciertos puntos de red*, cualquier intento de acceso desde otro punto puede marcarse como **sospechoso**.

🔍 Definiendo la Línea Base

- La **línea base** es el conjunto de comportamientos normales o permitidos.
- Puede incluir:
 - IPs autorizadas.
 - Usuarios frecuentes.
 - Servicios accedidos normalmente.
 - Tráfico de red habitual (puertos 80, 443).

Si de pronto aparecen intentos de conexión a puertos no usuales (23, 25, 8080), eso podría marcarse como **tráfico anómalo**.

🛡️ Indicadores de Compromiso (IoC)

Una vez definida la línea base, es posible comparar y detectar análisis de **IoC**. Ejemplo:

- Un usuario que intenta autenticarse desde una PC no habitual.
- Uso de credenciales que no son comunes para ese host.



💡 Herramientas de Monitoreo y Respuesta

⚖️ Security Onion

- Distribución basada en herramientas libres de **defensa**.
- Incluye IDS, firewall, herramientas de análisis de tráfico, entre otros.
- Similar a Kali Linux, pero para la defensa.
- Puede implementarse en entornos de **producción**.

⚙️ Preparación de Equipos de Respuesta

- No basta con herramientas; se necesita **formación continua**.
- La preparación implica:
 - Capacitación.
 - Entrenamiento práctico.
 - Uso adecuado de las herramientas.

🚫 Tipos de Incidentes

Una vez detectado un evento, se debe **clasificar**:

- **DDoS**: Negación de servicio.
- **Accesos no autorizados**.
- **Pruebas controladas**: Ej. ejercicios internos de seguridad como pruebas de penetración (pentest).

🌐 Comunicación en Pruebas Controladas

- Se debe notificar a los equipos involucrados:
 - Ejemplo: "Realizaremos un escaneo de 10 PM a 12 AM".
 - Esto evita falsas alarmas y respuestas innecesarias.

🚧 Consideraciones en Ejercicios Tipo Red Team

- En pruebas **Red Team**, la idea es simular un ataque real, por lo tanto **no se notifica con anticipación**.
- El SOC debe detectar la actividad como si fuera real, lo que prueba su capacidad real de detección y respuesta.

Un buen sistema de seguridad informática se basa en la capacidad de **detectar desviaciones**, **clasificarlas** adecuadamente y **responder con rapidez y eficacia**. Para ello, es clave combinar:

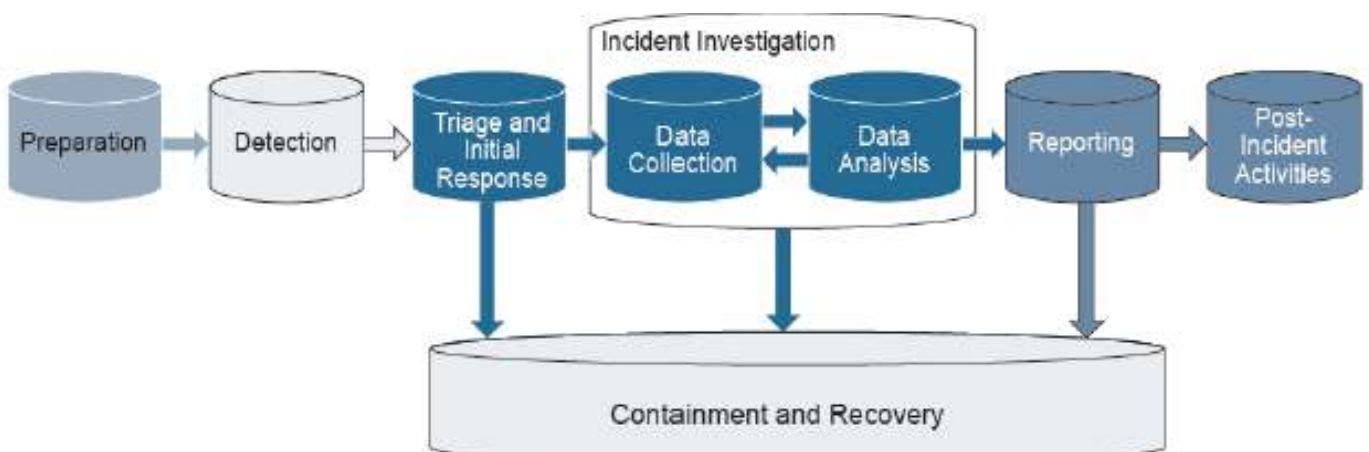
- 🖋️ Procesos bien definidos.
- ⚙️ Herramientas eficientes.
- 💪 Personal capacitado y entrenado.

🔄 Ciclo de respuesta a incidentes

◆ El objetivo es no ser detectado

En ejercicios tipo *Red Team*, la idea es que el ataque no sea detectado. Esto es diferente a ejercicios controlados o simulados en los que el equipo de seguridad está al tanto de la actividad.

Línea de tiempo del Proceso de Respuesta de Incidentes



1. Preparation (Preparación)

En esta fase, la organización se prepara ante posibles incidentes mediante políticas de seguridad, procedimientos, herramientas de monitoreo, entrenamiento del personal y simulacros. El objetivo es **minimizar riesgos y tiempos de respuesta**.

2. Detection (Detección)

Aquí se identifican posibles incidentes a través de sistemas como IDS/IPS, antivirus, SIEM o alertas de comportamiento inusual. Es crucial una **detección temprana** para que el daño sea menor.

3. Triage and Initial Response (Clasificación y respuesta inicial)

Una vez detectado un posible incidente, se clasifica según su gravedad y urgencia. El equipo responde inicialmente para **limitar el impacto** inmediato y decide si el incidente requiere una investigación más profunda.

Fase de *Triage* e Investigación

1. Triage inicial

Se realiza una **clasificación inicial del incidente**. Si amerita, se da una **respuesta inmediata**. Si no, se deriva a la siguiente etapa:

4. Incident Investigation (Investigación del incidente)

Esta etapa tiene tres subfases:

- **Data Collection:** Se recopilan evidencias digitales, registros, archivos afectados, tráfico de red, etc.
- **Data Analysis:** Se analiza esta información para determinar **qué pasó, cómo, cuándo y quién** lo hizo.
- Ambas fases están conectadas en bucle, ya que el análisis puede requerir más datos conforme avanza la investigación.

Containment and Recovery (Contención y recuperación)

Durante y después de la investigación, se aplican medidas para contener el incidente (por ejemplo, desconectar equipos, bloquear cuentas) y se inicia la recuperación de los sistemas afectados. El propósito es **restablecer la operación normal sin propagar el daño**.

2. Investigación

Aquí se:

- **Recopila más información**
- Se hace un **análisis técnico**
- Se toman **decisiones de contención y recuperación**

El objetivo es **cortar la amenaza** (contención) y **restaurar sistemas o servicios afectados** (recuperación).



5. Reporting (Informe)

Se elabora un informe con los hallazgos de la investigación, el impacto del incidente, las acciones realizadas y las recomendaciones. Este documento es clave para la toma de decisiones y puede ser usado como evidencia en auditorías o juicios.



Reportes y lecciones aprendidas

Una de las etapas más importantes, aunque poco valorada, es la **elaboración del informe** del incidente. Este reporte permite documentar:

- Qué pasó
- Cómo se resolvió
- **Qué se aprendió**

Esto alimenta la fase inicial de **preparación** para que la organización esté lista para el siguiente incidente, que inevitablemente ocurrirá.



6. Post-Incident Activities (Actividades posteriores al incidente)

Después del incidente, se revisan las lecciones aprendidas, se actualizan políticas, se refuerzan controles y se forma al personal. Esto ayuda a **mejorar la resiliencia y evitar incidentes similares** en el futuro.

Este ciclo no es estrictamente lineal: puede haber retrocesos y repeticiones entre fases. En conjunto, permite a una organización responder con eficacia y madurez ante amenazas de ciberseguridad.

Categorización de incidentes

Category Number	Name	Description
0	Exercise	Se utiliza cuando se realiza un ejercicio aprobado, como una prueba de penetración autorizada.
1	Unauthorized Access	Esto representa cuando una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso de un cliente.
2	Denial of Service (DoS)	Se utiliza cuando un ataque impide o perjudica con éxito la funcionalidad normal autorizada de redes, sistemas o aplicaciones al agotar los recursos.
3	Malicious Code	Identifica cuándo se instala correctamente software malicioso, como un virus, gusano, troyano u otra entidad maliciosa basada en código, que infecta un sistema operativo o una aplicación.
4	Scans/Probes/ Attempted Access	Esto incluye cualquier actividad que busque acceder o identificar un equipo cliente, abrir puertos, protocolos, servicios o cualquier combinación para un futuro ataque.
5	Investigation	Esto incluye incidentes no confirmados que son una actividad potencialmente maliciosa o anómala que la entidad informante considera que justifica una revisión adicional

Fuente: [BOOK] *Security Operations Center: Building, Operating, and Maintaining your SOC* (Muniz, 2015)

<https://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052014>

Categorización de incidentes

Un incidente puede clasificarse según su naturaleza:

1. **Acceso no autorizado**
2. **Negación de servicio (DoS/DDoS)**
3. **Código malicioso (virus, malware, ransomware)**

4. **Escaneos sospechosos**
5. **Investigación:** cuando el incidente es **aún desconocido**

Severidad de incidentes

Level	Description
High	Incidentes que tienen un impacto grave en las operaciones
Medium	Incidentes que tienen un impacto significativo, o el potencial de tener un impacto grave, en las operaciones
Low	Incidentes que tienen un impacto mínimo con el potencial de un impacto significativo o grave en las operaciones

También se evalúa la **severidad**:

- **Baja:** No tiene impacto real.
- **Media:** Afecta solo una parte no crítica.
- **Alta:** Impacta **directamente** las operaciones, bases de datos, aplicaciones, redes, etc.

👉 Por ejemplo: un simple escaneo puede convertirse en un evento **crítico** si revela o explota una vulnerabilidad en sistemas sensibles

Impacto y evolución de los ataques

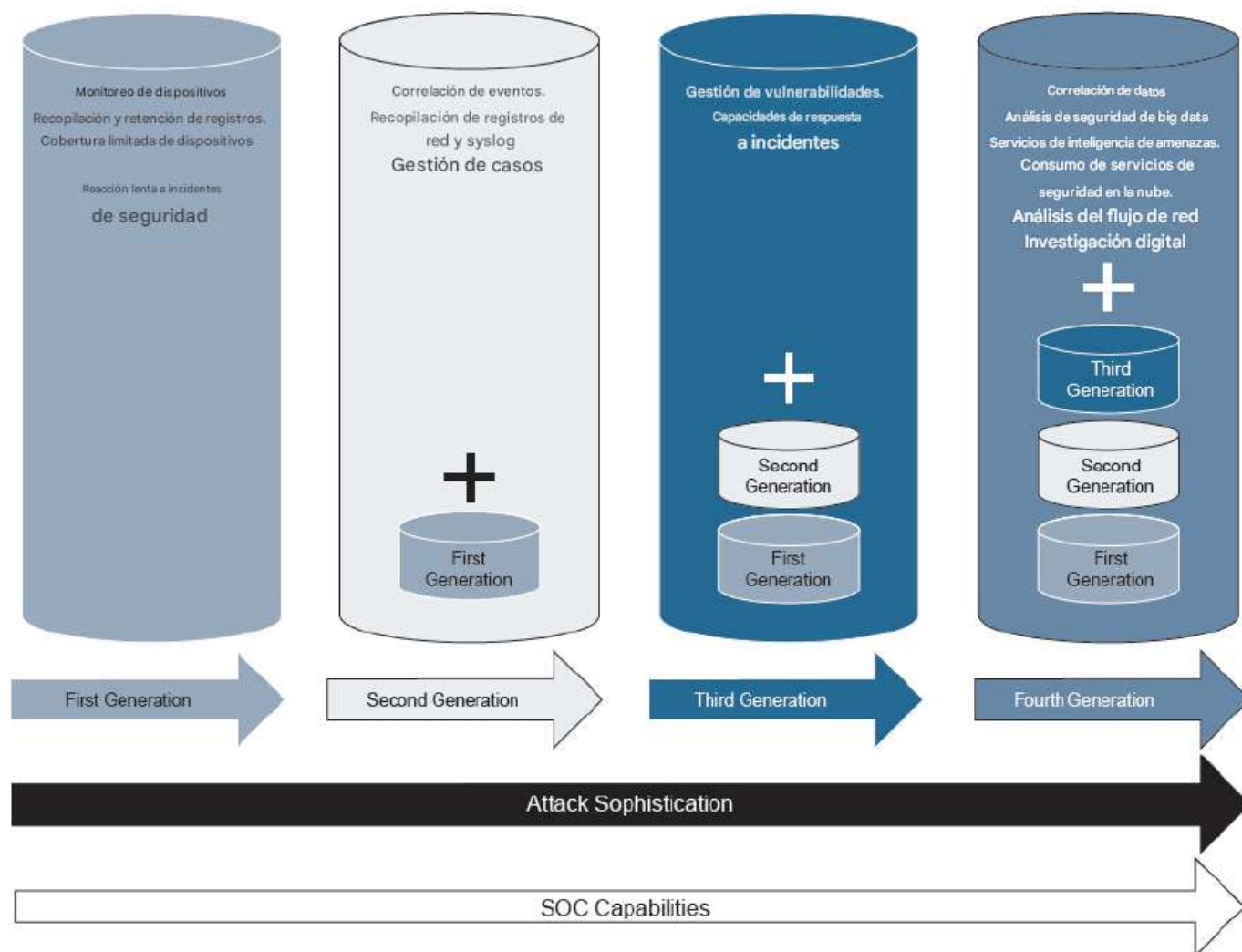
Cuando un incidente **aparentemente menor** escala, puede ocasionar consecuencias graves.

💡 *Ejemplo: un escaneo simple puede, sin control, **bajar todos los servidores**, afectando directamente la **continuidad operativa**. Esto demuestra que el **impacto no solo depende del ataque en sí**, sino de **qué tan crítico es el sistema afectado**.*

Generaciones de SOC

🚀 Evolución de los SOC (Security Operations Centers)

A medida que los **ataques se vuelven más sofisticados**, también deben evolucionar las **defensas**. Esta evolución ha dado lugar a **cuatro generaciones** de SOC, cada una con capacidades incrementadas:




la **evolución de los Centros de Operaciones de Seguridad (SOC)** a través de cuatro generaciones, y cómo han ido mejorando sus capacidades en respuesta al aumento en la sofisticación de los ciberataques.

Aquí te lo explico por partes:

Primera Generación

Primera Generación: SOC Básico

- **Capacidades:** Monitoreo de dispositivos, recolección y retención de logs.
- **Limitaciones:** Cobertura limitada, reacción lenta a incidentes de seguridad.
-  **Problema principal:** No detecta amenazas avanzadas ni correlaciona eventos complejos.

Primera generación:

- Recolección **manual de logs**
- Reacción **lenta**
- No hay correlación de eventos
- Se basa en la observación directa: *"Algo pasó, revisa el log"*

 **Limitación:** el análisis es reactivo y **poco eficiente** frente al volumen masivo de datos.

- El equipo de TI, asumía las funciones y servicios de un SOC.
- No se tenía un entrenamiento en el manejo de incidentes de seguridad de la información / seguridad informática.
- Las operaciones de seguridad no se realizaban por un SOC formal, sino a través del personal de TI.
- Uso de mensajes Syslog y SNMP, generalmente sin cifrar.
- No se utiliza un SIEM (Sistema de Gestión de Eventos y Seguridad de Información)
- La revisión de logs locales es una práctica común y manual post-incidente.

Segunda Generación

Segunda generación:

- Se añaden herramientas de **correlación de eventos**
- **Gestión básica de casos y triaje**

- Se recolectan logs de múltiples fuentes (**red, sistema, aplicaciones**)

✅ **Ventaja clave:** se puede **detectar patrones sospechosos** conectando eventos aparentemente aislados.

🔗 **Ejemplo:** Un acceso sospechoso desde una IP desconocida + intento de fuerza bruta + acceso a una base de datos → correlación que activa una alerta.

⚙️ Segunda Generación: SOC Correlacional


- **Agrega:** Correlación de eventos, análisis de logs de red y syslog, gestión de casos.
 - **Mejora:** Se comienza a identificar patrones de ataque mediante correlaciones automáticas.
 - ✅ **Ventaja:** Respuesta un poco más proactiva.
 - Incluye **todas las capacidades de la primera generación.**
- Herramientas de SIEM emergentes: *netForensics*, *Network Intelligence* (adquirido por EMC), y *Cisco Security Monitoring, Analysis, and Response System* (MARS)
 - Los primeros proveedores de tales herramientas se centraron en la gestión de amenazas de seguridad (STM), también conocida como gestión de eventos de seguridad (SEM).
 - Esta función SEM finalmente se consolidó con la función de administración de información de seguridad (SIM) para producir lo que hoy se conoce como SIEM.
 - Uso de sistema de tickets para la gestión de casos relacionados a incidentes de seguridad.

Tercera Generación

🛡️ Tercera generación:

- Se incorpora **gestión de vulnerabilidades**
- Aparecen los equipos formales como **CERTs y CSIRTs**
- Se desarrolla una **capacidad de respuesta organizada y estructurada**

🛡️ Tercera Generación: SOC con Gestión de Vulnerabilidades

- **Agrega:** Gestión de vulnerabilidades y capacidades de respuesta a incidentes.
 - **Avance:** El SOC ya puede anticipar y mitigar amenazas, no solo detectarlas.
 -  **Ventaja:** Identificación y cierre de brechas antes de que se exploten.
 - Incluye capacidades de la **primera y segunda generación**.
- El equipo SOC maneja las tareas relacionadas con la gestión de vulnerabilidades, además de estar muy involucrado en la formalización y ejecución de tareas relacionadas con la respuesta a incidentes.
 - La gestión de la vulnerabilidad se refiere a la práctica en la que se descubren y confirman las vulnerabilidades, se evalúa su impacto, se identifican y ejecutan las medidas correctivas y se realiza un seguimiento y se informa de su estado hasta el cierre. Esta definición es similar a la utilizada en el estándar NIST SP 800-40.26
 - Algunas herramientas como Qualys, nCircle (adquirido en 2013 por Tripwire), y Rapid7 Nexpose, han evolucionado para facilitar la gestión de vulnerabilidades.

Cuarta Generación


Cuarta generación:

- Integración de **inteligencia de amenazas**
- **Análisis de big data**
- Uso de **IA (Inteligencia Artificial)**
- **Investigación forense digital**
- Monitoreo y análisis de tráfico en red

 Este nivel exige:

- Mayor especialización
- Equipos multidisciplinarios
- Herramientas automatizadas de última generación

Cuarta Generación: SOC Inteligente y Analítico

- **Agrega:** Correlación de datos a gran escala, análisis de seguridad con Big Data, servicios de inteligencia de amenazas, uso de servicios en la nube, análisis de flujo de red e investigación digital.
- **Avance clave:** El SOC ahora es predictivo, proactivo y basado en inteligencia.
-  **Ventaja:** Se anticipa a los ataques y responde rápidamente gracias al uso de herramientas avanzadas como IA y machine learning.
- Integra **todas las generaciones anteriores**.




Relación entre ataque y capacidad

- En la parte inferior, se ve que a medida que **los ataques se vuelven más sofisticados (flecha negra)**, las **capacidades del SOC deben evolucionar (flecha blanca)**.
- Si el SOC no evoluciona, queda obsoleto ante amenazas modernas.

- De la correlación en SIEM a la seguridad de Big Data.
- El análisis de seguridad de Big Data se puede definir como "la capacidad de analizar gran cantidad de datos durante largos períodos de tiempo para descubrir amenazas y luego presentar y visualizar los resultados"
- Un ejemplo del uso de big data es ingerir grandes amenazas de inteligencia sobre ataques vistos en todo el mundo en lugar de limitar la correlación de eventos a amenazas internas.
- El SOC está utilizando las nuevas tecnologías para el análisis forense y para identificar fallas en la red.


Funciones de los Especialistas en Seguridad

En la ciberseguridad moderna, encontramos distintos roles clave como:

-  **Analista forense:** se encarga de investigar incidentes, identificar causas y preservar evidencia digital.
-  **Analista de tráfico de red:** analiza flujos de red y detecta patrones inusuales o potenciales amenazas.
-  **Analista de amenazas:** estudia malware, campañas de spam, y otras actividades maliciosas globales.




Estos perfiles están directamente vinculados a funciones prácticas dentro de un **SOC (Security Operations Center)**.

Recomendación Académica

 **Atención** para **exámenes:**
En evaluaciones suelen incluirse **casos o ejemplos**, y se pedirá reconocer **a qué función o perfil profesional** corresponde la actividad. Por eso, es **importante leer bien las descripciones** de cada perfil.

Visualización en Tiempo Real de Ataques

Puedes observar ataques cibernéticos **en tiempo real** desde sitios web especializados que muestran:


-  Localización de ataques
-  Tipo de malware o spam
-  Origen y destino del tráfico malicioso


Herramientas sugeridas:

- <https://cybermap.kaspersky.com>
- <https://www.digitalattackmap.com>
- **Talos (Cisco)**
- **Checkpoint ThreatCloud**
- **Fortinet Threat Map**



Cada uno muestra datos recopilados a partir de **sensores globales** y **agentes instalados en miles de dispositivos**.

Reflexión crítica


 **Pregunta** **clave:**
¿Cómo sabes si tu router u otro dispositivo está compartiendo información con estos fabricantes?

 **Posibilidad real:** Puede estar enviando datos no solo sobre ataques, sino también **información de tráfico interno**, lo cual plantea preocupaciones sobre **privacidad y control**.


Anuncios Finales de Clase

- Hoy se **suspende la clase** por una reunión del docente a las 12:30 h.
 - Quedan **pendientes dos temas**:
 1.  **Suscripciones** (ya está siendo preparado por un grupo).
 2.  **Seguridad en redes operacionales** (se compartirá el material, tema principalmente conceptual).
-

Clase práctica del jueves

 *Temas a repasar:*

- **Protocolos**
- **Conceptos clave de sistemas operativos**
- **Relación entre protocolos y seguridad**

 **Objetivo:** Consolidar lo aprendido en la unidad, enfocándose en cómo estos elementos contribuyen a la ciberseguridad.

RESUMEN COMPLETO DE LA CLASE SOBRE CIBERSEGURIDAD

Roles en un SOC (Centro de Operaciones de Seguridad)

1. **Analista Forense:** Investiga incidentes de seguridad, recolecta evidencia digital y analiza causas.
2. **Analista de Tráfico de Red:** Monitorea los flujos de datos para detectar actividades anómalas.
3. **Analista de Amenazas:** Estudia campañas de malware, phishing y amenazas persistentes.

Estos perfiles son esenciales en un **SOC**, cuya misión es proteger los activos digitales de una organización.

Herramientas para Visualizar Ciberataques en Tiempo Real

- Plataformas como **Talos (Cisco)**, **Checkpoint**, **Fortinet**, **Kaspersky CyberMap** y **Digital Attack Map** muestran:

- Tipo de ataque (malware, spam, DDoS, etc.)
- Ubicación geográfica
- Comportamiento de amenazas globales

Estos datos provienen de sensores y agentes conectados a miles de dispositivos.

Uso Ético y Crítico de Estas Herramientas

Los estudiantes deben aprender a **interpretar esta información** sin caer en una falsa sensación de seguridad.

También deben **cuestionar**: ¿Mi router comparte datos? ¿Qué tipo de información puede enviar?

Preparación para Evaluaciones

Es importante **identificar casos prácticos** y saber relacionarlos con el **perfil profesional adecuado** (forense, tráfico, amenazas, etc.).

Muchas preguntas de examen se basan en **situaciones reales o hipotéticas**.

Temas Pendientes

Se suspendió la clase por una reunión. Sin embargo, quedaron pendientes:

1. **Suscripciones** (tema asignado a un grupo)
2. **Seguridad en redes operacionales** (se entregará material)
3. **Clase práctica del jueves**: revisión de protocolos, sistemas operativos y su aplicación en seguridad informática.

PALABRAS CLAVE Y SIGNIFICADOS

Palabra Clave	Significado
SOC (<i>Security Operations Center</i>)	Centro donde se monitorean, detectan y responden incidentes de seguridad informática.
Forense digital	Rama de la ciberseguridad encargada de analizar evidencia electrónica tras un incidente.
Phishing	Suplantación de identidad mediante correos o mensajes falsos para robar datos.
Malware	Software malicioso diseñado para causar daño, robar información o tomar control de sistemas.

Agente	Programa que recopila datos de una máquina para enviarlos a un sistema central de análisis.
Correlación de eventos	Técnica para relacionar sucesos aparentemente aislados y detectar ataques o anomalías.
Línea base	Comportamiento habitual esperado de una red o sistema, usado para detectar anomalías.
Falso positivo	Alerta de seguridad que se activa sin que exista realmente una amenaza.
Falso negativo	No se detecta una amenaza real. Muy peligroso en ciberseguridad.
Command and Control (C2)	Sistema de control remoto usado por atacantes para mantener presencia en el sistema víctima.
APT (Advanced Persistent Threat)	Amenaza persistente y avanzada, difícil de detectar, mantenida por largo tiempo dentro del sistema.
Mitre ATT&CK	Marco de referencia que documenta tácticas y técnicas utilizadas por atacantes en diferentes etapas.
Triaje	Clasificación inicial de incidentes según su severidad o tipo.
Ejercicio de Red Team	Prueba ofensiva (simulación de ataque real) para evaluar la seguridad de una organización.
SIEM	Sistema de Gestión de Información de Seguridad que recoge, analiza y correlaciona logs y eventos.